

COSE Working Group
Internet-Draft
Intended status: Informational
Expires: 12 November 2026

L. Liao
NIO
G. Selander
J. Preu Mattsson
Ericsson
11 May 2026

Test Vectors for CBOR Encoded X.509 (C509) Certificates
draft-ietf-cose-c509-test-vectors-01

Abstract

This document contains examples of CBOR-encoded X.509 (C509) certificates, certification requests, and certification 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 12 November 2026.

Copyright Notice

Copyright (c) 2026 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction	7
1.1. Terminology	9
2. CA Certificate	9
2.1. Private Key	9
2.2. X.509 Certificate	9
2.3. C509 Type 3 Certificate	10
2.4. C509 Type 2 Certificate	11
3. Certificates With Different Subject Public Keys	11
3.1. RSA Public Key With Public Exponent 65537	11
3.1.1. Private Key	12
3.1.2. X.509 Certificate	12
3.1.3. C509 Type 3 Certificate	13
3.1.4. C509 Type 2 Certificate	14
3.2. RSA Public Key With Public Exponent 4294967297	15
3.2.1. Private Key	15
3.2.2. X.509 Certificate	16
3.2.3. C509 Type 3 Certificate	17
3.2.4. C509 Type 2 Certificate	18
3.3. Weierstrass EC Public Key On Curve secp256r1	19
3.3.1. Private Key	20
3.3.2. X.509 Certificate	20
3.3.3. C509 Type 3 Certificate	21
3.3.4. C509 Type 2 Certificate	22
3.4. Compressed Weierstrass EC Public Key On Curve secp256r1	23
3.4.1. Private Key	24
3.4.2. X.509 Certificate	24
3.4.3. C509 Type 3 Certificate	25
3.4.4. C509 Type 2 Certificate	26
3.5. Weierstrass EC Public Key On Curve secp384r1	27
3.5.1. Private Key	28
3.5.2. X.509 Certificate	28
3.5.3. C509 Type 3 Certificate	29
3.5.4. C509 Type 2 Certificate	30
3.6. Weierstrass EC Public Key On Curve secp521r1	32
3.6.1. Private Key	32
3.6.2. X.509 Certificate	32
3.6.3. C509 Type 3 Certificate	34
3.6.4. C509 Type 2 Certificate	35
3.7. Weierstrass EC Public Key On Curve sm2p256v1	37
3.7.1. Private Key	38
3.7.2. X.509 Certificate	38
3.7.3. C509 Type 3 Certificate	39
3.7.4. C509 Type 2 Certificate	40
3.8. Weierstrass EC Public Key On Curve brainpoolP256r1	42
3.8.1. Private Key	42

3.8.2.	X.509 Certificate	42
3.8.3.	C509 Type 3 Certificate	44
3.8.4.	C509 Type 2 Certificate	45
3.9.	Weierstrass EC Public Key On Curve brainpoolP384r1	47
3.9.1.	Private Key	47
3.9.2.	X.509 Certificate	48
3.9.3.	C509 Type 3 Certificate	50
3.9.4.	C509 Type 2 Certificate	50
3.10.	Weierstrass EC Public Key On Curve brainpoolP512r1	52
3.10.1.	Private Key	53
3.10.2.	X.509 Certificate	53
3.10.3.	C509 Type 3 Certificate	55
3.10.4.	C509 Type 2 Certificate	55
3.11.	Weierstrass EC Public Key On Curve frp256v1	57
3.11.1.	Private Key	58
3.11.2.	X.509 Certificate	58
3.11.3.	C509 Type 2 Certificate	60
3.12.	Montgomery EC Public Key On Curve X25519	62
3.12.1.	Private Key	62
3.12.2.	X.509 Certificate	62
3.12.3.	C509 Type 3 Certificate	63
3.12.4.	C509 Type 2 Certificate	64
3.13.	Montgomery EC Public Key On Curve X448	66
3.13.1.	Private Key	66
3.13.2.	X.509 Certificate	67
3.13.3.	C509 Type 3 Certificate	68
3.13.4.	C509 Type 2 Certificate	69
3.14.	Edwards EC Public Key On Curve ED25519	71
3.14.1.	Private Key	71
3.14.2.	X.509 Certificate	71
3.14.3.	C509 Type 3 Certificate	73
3.14.4.	C509 Type 2 Certificate	74
3.15.	Edwards EC Public Key On Curve ED448	76
3.15.1.	Private Key	77
3.15.2.	X.509 Certificate	77
3.15.3.	C509 Type 3 Certificate	78
3.15.4.	C509 Type 2 Certificate	79
4.	Certificates With Different Signature Algorithms	81
4.1.	RSASSA-PKCS1-v1_5 With SHA-1	81
4.1.1.	Private Key	81
4.1.2.	X.509 Certificate	81
4.1.3.	C509 Type 3 Certificate	82
4.1.4.	C509 Type 2 Certificate	83
4.2.	ECDSA With SHA1	84
4.3.	ECDSA With SHA256	84
4.4.	ECDSA With SHA384	84
4.5.	ECDSA With SHA512	85
4.6.	ECDSA With SHAKE128	85

4.7.	ECDSA With SHAKE256	85
4.8.	Unsigned	85
4.9.	SM2 With SM3	85
4.10.	Ed25519	85
4.11.	Ed448	85
4.12.	ECDH PoP With SHA-256 And HMAC-SHA256	85
4.13.	ECDH PoP With SHA-384 And HMAC-SHA384	86
4.14.	ECDH PoP With SHA-512 And HMAC-SHA512	86
4.15.	RSASSA-PKCS1-v1_5 With SHA-256	86
4.16.	RSASSA-PKCS1-v1_5 With SHA-384	86
4.17.	RSASSA-PKCS1-v1_5 With SHA-512	86
4.17.1.	Private Key	86
4.17.2.	X.509 Certificate	86
4.17.3.	C509 Type 3 Certificate	88
4.17.4.	C509 Type 2 Certificate	88
4.18.	RSASSA-PSS With SHA-256	89
4.18.1.	Private Key	89
4.18.2.	X.509 Certificate	89
4.18.3.	C509 Type 3 Certificate	91
4.18.4.	C509 Type 2 Certificate	92
4.19.	RSASSA-PSS With SHA-384	93
4.19.1.	Private Key	93
4.19.2.	X.509 Certificate	93
4.19.3.	C509 Type 3 Certificate	95
4.19.4.	C509 Type 2 Certificate	96
4.20.	RSASSA-PSS With SHA-512	97
4.20.1.	Private Key	97
4.20.2.	X.509 Certificate	98
4.20.3.	C509 Type 3 Certificate	99
4.20.4.	C509 Type 2 Certificate	100
4.21.	RSASSA-PSS With SHAKE128	101
4.21.1.	Private Key	101
4.21.2.	X.509 Certificate	101
4.21.3.	C509 Type 3 Certificate	103
4.21.4.	C509 Type 2 Certificate	103
4.22.	RSASSA-PSS With SHAKE256	104
4.22.1.	Private Key	104
4.22.2.	X.509 Certificate	104
4.22.3.	C509 Type 3 Certificate	106
4.22.4.	C509 Type 2 Certificate	107
5.	Certificates With Different RDN Attributes	108
5.1.	One RDN Attribute CommonName With EUI-48	108
5.2.	One RDN Attribute CommonName With EUI-64	108
5.3.	One RDN Attribute CommonName With Even Number Of Lowercase Hex Letters	109
5.4.	One RDN Attribute CommonName With Other Text	109
5.5.	Empty Subject	109
5.6.	Subject With RDN Attribute Business Category	109

5.7.	Subject With RDN Attribute Country	109
5.8.	Subject With RDN Attribute Directory Management Domain Name	109
5.9.	Subject With RDN Attribute DN Qualifier	109
5.10.	Subject With RDN Attribute Domain Component	110
5.11.	Subject With RDN Attribute Email Address	110
5.12.	Subject With RDN Attribute Generation Qualifier	110
5.13.	Subject With RDN Attribute Given Name	110
5.14.	Subject With RDN Attribute Initials	110
5.15.	Subject With RDN Attribute Jurisdiction Country	110
5.16.	Subject With RDN Attribute Jurisdiction Locality	110
5.17.	Subject With RDN Attribute Jurisdiction State Or Province	110
5.18.	Subject With RDN Attribute Locality	111
5.19.	Subject With RDN Attribute Name	111
5.20.	Subject With RDN Attribute Organization	111
5.21.	Subject With RDN Attribute Organizational Unit	111
5.22.	Subject With RDN Attribute Organization Identifier	111
5.23.	Subject With RDN Attribute Postal Code	111
5.24.	Subject With RDN Attribute Pseudonym	111
5.25.	Subject With RDN Attribute Serial Number	111
5.26.	Subject With RDN Attribute State	112
5.27.	Subject With RDN Attribute Street	112
5.28.	Subject With RDN Attribute Surname	112
5.29.	Subject With RDN Attribute Telephone Number	112
5.30.	Subject With RDN Attribute Title	112
5.31.	Subject With RDN Attribute Unstructured Address	112
5.32.	Subject With RDN Attribute Unstructured Name	112
5.33.	Subject With RDN Attribute User Id	112
6.	Certificates With Different Extensions	113
6.1.	Empty Extensions	113
6.2.	One Extension: Non-Critical keyUsage	113
6.3.	One Extension: Critical keyUsage	113
6.4.	Authority Information Access	113
6.5.	Authority Key Identifier	113
6.6.	ASIdentifiers And ASIdentifiers V2	113
6.7.	Basic Constraints	113
6.8.	Certificate Policies	114
6.9.	CRL Distribution Points and Freshest CRL	114
6.10.	Extended Key Usage	114
6.11.	Inhibit anyPolicy	114
6.12.	Issuer Alternative Name	114
6.13.	IPAddrBlocks and IPAddrBlocks V2	114
6.14.	Name Constraints	115
6.15.	OCSP No Check	115
6.16.	Policy Constraints	115
6.17.	Policy Mappings	115
6.18.	Subject Alternative Name	115

6.19. Subject Directory Attributes	116
6.20. Subject Information Access	116
6.21. Subject Key Identifier	116
6.22. TLS Features	116
7. X.509 Certificate With Unconvertible RDN Attributes And Extensions	116
7.1. Private Key	116
7.2. X.509 Certificate	116
7.3. C509 Type 3 Certificate	118
8. Certification Requests With Different Signature Algorithms	120
8.1. ECDSA With SHA256	120
8.1.1. Private Key	120
8.1.2. X.509 Certification Request	120
8.1.3. C509 Type 3 Certification Request	121
8.1.4. C509 Type 2 Certification Request	121
8.2. ECDSA With SHA384	122
8.2.1. Private Key	122
8.2.2. X.509 Certification Request	122
8.2.3. C509 Type 3 Certification Request	123
8.2.4. C509 Type 2 Certification Request	124
8.3. ECDH PoP With SHA-256 And HMAC-SHA256	124
8.3.1. Private Key	125
8.3.2. X.509 Certification Request	125
8.3.3. C509 Type 3 Certification Request	125
8.3.4. C509 Type 2 Certification Request	126
8.4. ECDH PoP With SHA-384 And HMAC-SHA384	127
8.4.1. Private Key	127
8.4.2. X.509 Certification Request	127
8.4.3. C509 Type 3 Certification Request	128
8.4.4. C509 Type 2 Certification Request	128
8.5. ECDH PoP With SHA-512 And HMAC-SHA512	129
8.5.1. Private Key	129
8.5.2. X.509 Certification Request	130
8.5.3. C509 Type 3 Certification Request	131
8.5.4. C509 Type 2 Certification Request	131
8.6. Unsigned PoP With X25519 Key	132
8.6.1. Private Key	132
8.6.2. X.509 Certification Request	132
8.6.3. C509 Type 3 Certification Request	133
8.6.4. C509 Type 2 Certification Request	133
8.7. Unsigned PoP With X25519 Key And Cert	134
8.7.1. Private Key	134
8.7.2. X.509 Certification Request	134
8.7.3. C509 Type 3 Certification Request	135
8.7.4. C509 Type 2 Certification Request	136
9. Certification Requests With Different CR Attributes	138
9.1. With Empty CR Attributes	138
9.2. With challengePassword Attribute	138

9.3. With extensionRequest Attribute	138
9.4. With privateKeyPossessionStatement Attribute	138
10. Certification Request Templates	138
10.1. All Fields Set to "undefined" Where Possible	138
10.2. With One Element in Each Field	139
10.3. Complex Template	140
11. Security Considerations	142
12. Privacy Considerations	143
13. IANA Considerations	143
14. References	143
14.1. Normative References	143
14.2. Informative References	143
Acknowledgments	144
Authors' Addresses	144

1. Introduction

This document contains examples of X.509 certificates, certification requests, and certification request templates encoded in CBOR [RFC8949] according to the C509 specification [I-D.ietf-cose-cbor-encoded-cert]. It complements the C509 specification by providing readable examples that illustrate the encodings of certificate and certification request fields and that can be used to test interoperability between C509 implementations.

The examples are shown in multiple encodings and formats: X.509 certificates and certification requests in PEM format, and C509 certificates and certification requests in plain hexadecimal and annotated forms.

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` (called type 3 in this document) is a reversible CBOR encoding of an X.509 certificate, in which the `issuerSignatureValue` field of the C509 certificate contains the `signatureValue` field of the X.509 certificate, that is, the digital signature computed over the ASN.1 DER encoding.
- * `c509CertificateType = 02` (called type 2 in this document) differs from type 3 only in this value and in that the `issuerSignatureValue` field of the C509 certificate contains the signature over the TBSCertificate of the C509 certificate, that is, the digital signature computed over the CBOR encoding.

The examples also include two types of C509 certification requests, called type 2 and type 3 in this document, distinguished by the value of the `c509CertificationRequestType` field.

Following [I-D.ietf-cose-cbor-encoded-cert], the C509 plain hex contains the `~C509Certificate`, `~C509CertificationRequest`, and `~C509CertificationRequestTemplate`, that is, the unwrapped CBOR Sequence [RFC8742]. These can readily be converted to CBOR diagnostic notation (see Section 8 of [RFC8949]) using the CBOR Playground [CborMe]. Note that CBOR Sequences require selecting the `cborseq` option in the CBOR Playground.

Private keys are also provided to enable the creation of signatures and the verification of ECDH proof of possession. The keys printed in these examples are not secret and MUST NOT be used for any purpose other than testing.

The examples are structured as follows:

- * Section 2 contains a CA certificate used in later sections.
- * Section 3 contains certificates with different subject public key types, including RSA, Weierstrass EC, Edwards EC, and Montgomery EC keys.
- * Section 4 contains certificates with different signature and proof-of-possession algorithms and points to the sections where those algorithms are encoded.
- * Section 5 contains certificates with different RDN attributes and points to the sections where those attributes are encoded.
- * Section 6 contains certificates with different extensions and points to the sections where those extensions are encoded.
- * Section 7 provides examples of certificates with RDN attributes or extensions for which no dedicated CBOR encoding has been defined and for which generic constructs such as CBOR OID [RFC9090] are used.
- * Section 8 provides examples of certification requests with different signature or proof-of-possession algorithms.
- * Section 9 provides examples of certification requests with different CR attributes.
- * Section 10 provides examples of certification request templates.

Editor's note: The current version does not include keys or signatures for post-quantum algorithms. These 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

- * The CA uses an Ed25519 public key because the resulting signature is compact.
- * Signature algorithm: unsigned
- * Key: Ed25519

2.1. Private Key

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

2.2. X.509 Certificate

PEM content (245 bytes):

```
-----BEGIN CERTIFICATE-----
MIHyMIHgoAMCAQICAQEwCgYIKwYBBQUHBIQWEjEQMA4GA1UEAwHdGVzdCBjYTAe
Fw0yNTAxMDEwMDAwMDBaFw0yNjEyMzEyMzU5NTlaMBIxEDAOBgNVBAMMB3Rlc3Qg
Y2EwKjAFBgMrZXADIBalBSsVtG2rwyWb8U7lHalYV0O6q73ZNnv6G23Mgw24aNW
MFQwHQYDVR0OBBYEFH/NuC0ElS4aNrkK83o88WbRXvkhMA4GA1UdDwEB/wQEAwIB
BjASBgNVHREECzAJggdhYmMuY29tMA8GA1UdEwEB/wQFMAMBAf8wCgYIKwYBBQUH
BiQDAQA=
-----END CERTIFICATE-----
```

Textual Representation:

Certificate:

Version: v3 (2)

Serial Number:

01

Issuer: CN=test ca

Validity:

Not Before: Wed Jan 01 01:00:00 CET 2025

Not After : Fri Jan 01 00:59:59 CET 2027

Subject: CN=test ca

Subject Public Key Info:

Public Key Algorithm: ED25519

Pub:

5a:94:14:ac:56:d1:b6:af:0c:96:6f:c5:3b:94:76:b5:c9:5d:

0e:ea:ae:f7:64:d9:ef:e8:6d:b7:32:0c:36:e1

X509v3 extensions:

X509v3 subjectKeyIdentifier:

7f:cd:b8:2d:04:95:2e:1a:36:b9:0a:f3:7a:3c:f1:66:d1:5e:f9:21

X509v3 keyUsage: critical

keyCertSign, cRLSign

X509v3 subjectAlternativeName:

DNS: abc.com

X509v3 basicConstraints: critical

CA: true, pathlen: null

Signature Algorithm: unsigned

Signature Value: <empty>

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 differences are the certificate type, the signature value, and the public key identifier.

Plain hex (96 bytes):

```
03410105F61A677485801A6B36EC7F67746573742063610C58205A9414AC56D1B6AF
0C966FC53B9476B5C95D0EEAAEF764D9EFE86DB7320C36E18801547FCDB82D04952E
1A36B90AF37A3CF166D15EF92121186003676162632E636F6D232040
```

Annotated hex:

- * See the annotated hex for the C509 type 2 certificate in Section 2.4. The only differences are the certificate type, the signature value, and the key identifiers.

2.4. C509 Type 2 Certificate

Plain hex (96 bytes):

```
02410105F61A677485801A6B36EC7F67746573742063610C58205A9414AC56D1B6AF
0C966FC53B9476B5C95D0EEAAEF764D9EFE86DB7320C36E18801540369D71F96FE12
58A746AC2B208E756E6D1D3ED921186003676162632E636F6D232040
```

Annotated hex:

```
0: 02          # [0]. certificate type=2
1: 41          # [1]. certificateSerialNumber=byte[1]
2: 01
3: 05          # [2]. signature alg=5: unsigned
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: 0C          # [7]. subjectPublicKeyAlg=12: Ed25519
24: 58 20       # [8]. subject public key=EC point=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: 0369D71F96FE1258A746AC2B208E756E6D1D3ED9
          # 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: 40          # [10]. signature value=byte[0]
```

3. Certificates With Different Subject Public Keys

3.1. RSA Public Key With Public Exponent 65537

* Self-signed certificate

- * RSA public key with public exponent 65537 ($= 2^{16} + 1$) and a 1024-bit modulus.
- * Signature algorithm: sha256WithRSAEncryption
- * NotAfter: null
- * Subject: a commonName containing an EUI-48 value
- * Extensions: a single non-critical keyUsage extension

3.1.1. Private Key

```
-----BEGIN PRIVATE KEY-----
MIICdgIBADANBgkqhkiG9w0BAQEFAASCAmAwggJcAgEAAoGBALgJL28EcmqSHPqy
0xOunS8Bx85GX6t9pix6XHP6zl/7ovHdgKKa3EM5nPyiInm4miZIEOW5JrteDT9y
enY+FgE/ifj+rFnQ+9leiwxSgn5UkPE7hMNjTonG0XMa5fGmD4jtEY0IDhqyyqUy
0GwvfSoIdN7k5rblcoP2R42vQlPbAgMBAAECgYAfuNGYyMLyFLJzEhzipERmd7ygi
KaY2+KcKlqLWCP7Gs6jAGQahwKDD46voLghUQ9oqTBTBjDsdY9ZTv+dU9lmyXRnR
8lQZxVmzFfZRZlyNBZE7NctjHlUMluejX08dp8ypFEZ8YUXydgwnVThyma6nwqeD
W2hAnP7S7LcisHs9/QJBAPJNe3l0Mqeq8Fwp4DL6opcnehT4qMe0d+/4nSIVodQc
iOJE752KYXslGZ0/+ETWNoBn8L7ZF09gjed/xtlSAEUCQQDCcHyiGcuNRfx6vTGo
8Su460/PF8ViALOUAZwPiFO+Fxp2kyWkK5DtKbCOXgeEPE2gcCFT1ztb/nusPJv
PJWfAkBMlrN0ZZv2veexYno90GulQZiec+iaRCnQyOeTuoZyTIZAMxpFvG+Dceho
jLO/qKrp94xKCW9xJg5wGJ5HppB9AkAVaKlQa+att0k3enltTKCzy7UN6GAjWlBr
i4HTc/9Efua6gn7MSfw0GEAEQq+nH9ZvWfoIs6RXwGyUi4cmGFWhAkEAjf207bsV
VUEhtJ3LEsgOatGg+8VfHIZuXxNNwxyIm2YactXDXpvs1FWRuNxomp44dtPmmb
bqJRmhxWlrumnw==
-----END PRIVATE KEY-----
```

3.1.2. X.509 Certificate

PEM content (464 bytes):

```
-----BEGIN CERTIFICATE-----
MIIBzDCCATWgAwIBAgICEjQwDQYJKoZIhvcNAQELBQAwIjEgMB4GA1UEAwwXMTIt
MzQtNTYtRkYtRkUtNzgtOTAtQUIwIBcNMjUwMTAyMDAwMDAwWhgPOTk5OTEyMzEy
MzU5NTlaMCIXIDAeBgNVBAMMFzEyLTM0LTU2LUZGLUZFLTc4LTkwLUFUMIGfMA0G
CSqGSIb3DQEBAQUAA4GNADCBiQKBgQC4CS9vBHJqkhz6stMTrp0vAcfORl+rfaYs
elxz+s5f+6Lx3YCimtxDOZz8oiJ5uJomSBDluSa7Xg0/cnp2PhYBP4n4/qxZ0Pvd
XosMUoJ+VJDxO4TDY06JxtFzGuXxpg+I7RGNCA4assqlMtBsL30qCHTe50a25XKD
9keNr0JT2wIDAQABow8wDTALBgNVHQ8EBAMCB4AwDQYJKoZIhvcNAQELBQADgYEA
GBLBJZ3E5ChTAXQA4d/ZO6GbIyvogslssZnHA80bdbg03D8/6USiLw/Y3ETDc+CS
dWtBTRsVWLv9DTEMWu54D2UQnp9jgoiuouE+mCvAhC00DjCAizYJ5yDk5xN93Vik
7jHXYl9hrTw2ey826BOcyJuxlfUfn9GMGf7LHRYs6Ok=
-----END CERTIFICATE-----
```

Textual Representation:

Certificate:

Version: v3 (2)

Serial Number:

12:34

Issuer: CN=12-34-56-FF-FE-78-90-AB

Validity:

Not Before: Thu Jan 02 01:00:00 CET 2025

Not After : Sat Jan 01 00:59:59 CET 10000

Subject: CN=12-34-56-FF-FE-78-90-AB

Subject Public Key Info:

Public Key Algorithm: 1.2.840.113549.1.1.1

Pub:

30:81:89:02:81:81:00:b8:09:2f:6f:04:72:6a:92:1c:fa:b2:
d3:13:ae:9d:2f:01:c7:ce:46:5f:ab:7d:a6:2c:7a:5c:73:fa:
ce:5f:fb:a2:f1:dd:80:a2:9a:dc:43:39:9c:fc:a2:22:79:b8:
9a:26:48:10:e5:b9:26:bb:5e:0d:3f:72:7a:76:3e:16:01:3f:
89:f8:fe:ac:59:d0:fb:dd:5e:8b:0c:52:82:7e:54:90:f1:3b:
84:c3:63:4e:89:c6:d1:73:1a:e5:f1:a6:0f:88:ed:11:8d:08:
0e:1a:b2:ca:a5:32:d0:6c:2f:7d:2a:08:74:de:e4:e6:b6:e5:
72:83:f6:47:8d:af:42:53:db:02:03:01:00:01

X509v3 extensions:

X509v3 keyUsage:

digitalSignature

Signature Algorithm: SHA256WITHRSA

Signature Value:

18:12:c1:25:9d:c4:e4:28:53:01:74:00:e1:df:d9:3b:a1:9b:
23:2b:e8:82:c9:6c:b1:99:c7:03:cd:1b:0d:b8:34:dc:3f:3f:
e9:44:a2:2f:0f:d8:dc:44:c3:73:e0:92:75:6b:41:4d:1b:15:
58:bb:fd:0d:31:0c:5a:ee:78:0f:65:10:9e:9f:63:82:88:ae:
a2:e1:3e:98:2b:c0:84:2d:34:0e:30:80:8b:36:09:e7:20:e4:
e7:13:7d:dd:58:a4:ee:31:d7:62:5f:61:ad:3c:36:7b:2f:36:
e8:13:9c:c8:9b:b1:95:f5:1f:37:d1:8c:19:fe:cb:1d:16:2c:
e8:e9

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 differences are 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 for the C509 type 2 certificate in Section 3.1.4. The only differences are the certificate type, the signature value, and the key identifiers.

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]. certificateSerialNumber=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=modulus=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 4294967297

- * Self-signed certificate
- * RSA public key with public exponent 4294967297 ($= 2^{32} + 1$) and a 1024-bit modulus
- * Signature algorithm: sha384WithRSAEncryption
- * Subject: a commonName containing an EUI-64 value
- * Extensions: a single critical keyUsage extension

3.2.1. Private Key

-----BEGIN PRIVATE KEY-----

```
MIICeQIBADANBgkqhkiG9w0BAQEFAASCAmMwggJfAgEAAoGBALgJL28EcmqSHPqy
0xOunS8Bx85GX6t9pix6XHP6zl/7ovHdgKKa3EM5nPyiInm4miZIEOW5JrteDT9y
enY+FgE/ifj+rFnQ+9leiwxSgn5UkPE7hMNjTonG0XMa5fGmD4jtEY0IDhqyyqUy
0GwvfSoIdN7k5rblcoP2R42vQlPbAgUBAAAAAQKBgE3mIbMMJlO/XyHBNfBtKWLe
6Sf+tlOecafT3HGmDHbZc+Z5ENXuCJw7troW2qozNNk23fNayknBxlqJjAgL0bD3
zwWk0SYJwFXQDUu/9D8RUas14eQfC5WUQGBAGuJVXDMYK7LoNulWvCD+KQIndBLN
u6wzYRMWmwq3BWtEFsLVAkEA8k17eXQyp6rwXCngMvqilyd6FPiox7R37/idIhWh
lByI4kTvnYphezUZnT/4RNY2gGfwvtkU72CNx3/G2VIARQJBAMJwfKIZy41EXHq9
MajxK7jrT88XxWIAS5QBnA+IU74XGnHaTJYqTkO0psI5eB4Q8TaBwIVPX0lv+e6w
8m88lZ8CQBsjKNy9t67rKHgi3j6OP6OnQKEawjrTJ6sxRPbHvKQ//Eqihnuv8M7Q
tKCYIIjm3lyHvyi7WJzb8lKtdzRQACKCQQCJ8eE96J22NQsKhaH2GYQaoyaJPTg0
hXXlJPXV3a7otceXpoWJldH7cYBf4vKpHlJlVn59TdmRXAvUH2P544ZzAkEAjf20
7bsVVUEhtJ3LEsgOatGg+8VfHIZuXxNNwxyIm2YactXDXpvfslFWRuNxomp44dt
PmmmbbqJrmhxWlrumnw==
```

-----END PRIVATE KEY-----

3.2.2. X.509 Certificate

PEM content (467 bytes):

-----BEGIN CERTIFICATE-----

```
MIIBzzCCATigAwIBAgICEjQwDQYJKoZIhvcNAQEMBQAwIjEgMB4GA1UEAwwXMTIt
MzQtNTYtNzgtOTAtQUItQ0QtRUYwHhcnMjUwMTAyMDAwMDAwWhcnMjYwMTAyMDAw
MDAwWjAiMSAwHgYDVQDDbCcxMi0zNC01Ni03OC05MC1BQilDRClFRjCB0TANBgkq
hkiG9w0BAQEFAAOBjwAwgYsCgYEAuAkvbWRYapIc+rLTE66dLwHHzkZfq32mLHpc
c/rOX/ui8d2AoprcQzmc/KIiebiaJkqG5bkmu14NP3J6dj4WAT+J+P6sWdD73V6L
DFKcflSQ8TuEw2NOicbRcxrl8aYPiO0RjQgOGrLKpTLQbC99Kgh03uTmtuVyg/ZH
ja9CU9sCBQEAAAABoxIwEDA0BgNVHQ8BAf8EBAMCB4AwDQYJKoZIhvcNAQEMBQAD
gYEAds76W8xddqZgQ+2qwuS/ule85K4HB5VkfEvyB/RphTFhZwUjLKCD97af01v7
7QQ62LJigojdL44ZyGwgx97itpr6CRuC76vbxau9+RyEWdFP+M+/bRD2jqWvrnR0
mIIQ2CmvG8Z+AaXf6kMKqgckKohtQwcBTt9sGkLgLQuJNSE=
```

-----END CERTIFICATE-----

Textual Representation:

Certificate:

Version: v3 (2)

Serial Number:

12:34

Issuer: CN=12-34-56-78-90-AB-CD-EF

Validity:

Not Before: Thu Jan 02 01:00:00 CET 2025

Not After : Fri Jan 02 01:00:00 CET 2026

Subject: CN=12-34-56-78-90-AB-CD-EF

Subject Public Key Info:

Public Key Algorithm: 1.2.840.113549.1.1.1

Pub:

30:81:8b:02:81:81:00:b8:09:2f:6f:04:72:6a:92:1c:fa:b2:
d3:13:ae:9d:2f:01:c7:ce:46:5f:ab:7d:a6:2c:7a:5c:73:fa:
ce:5f:fb:a2:f1:dd:80:a2:9a:dc:43:39:9c:fc:a2:22:79:b8:
9a:26:48:10:e5:b9:26:bb:5e:0d:3f:72:7a:76:3e:16:01:3f:
89:f8:fe:ac:59:d0:fb:dd:5e:8b:0c:52:82:7e:54:90:f1:3b:
84:c3:63:4e:89:c6:d1:73:1a:e5:f1:a6:0f:88:ed:11:8d:08:
0e:1a:b2:ca:a5:32:d0:6c:2f:7d:2a:08:74:de:e4:e6:b6:e5:
72:83:f6:47:8d:af:42:53:db:02:05:01:00:00:00:01

X509v3 extensions:

X509v3 keyUsage: critical

digitalSignature

Signature Algorithm: SHA384WITHRSA

Signature Value:

76:ce:fa:5b:cc:5d:76:a6:60:43:ed:aa:c2:e4:bf:ba:51:3c:
e4:ae:07:07:95:64:14:4b:f2:07:f4:69:85:31:61:67:05:23:
94:a0:83:f7:b6:9f:d3:5b:fb:ed:04:3a:d8:b2:62:82:88:dd:
2f:8e:19:c8:6c:20:c7:de:e2:b6:9a:fa:09:1b:82:ef:ab:db:
c5:ab:bd:f9:1c:84:59:d1:4f:f8:cf:bf:6d:10:f6:8e:a5:af:
ae:74:74:98:82:10:d8:29:af:1b:c6:7e:01:a5:df:ea:43:0a:
aa:07:24:2a:88:6d:43:07:01:4e:df:6c:1a:42:e0:2d:0b:89:
35:21

3.2.3. C509 Type 3 Certificate

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

Plain hex (297 bytes):

```
034212341818F61A6775D7001A69570A80D830481234567890ABCDEF00825880B809
2F6F04726A921CFAB2D313AE9D2F01C7CE465FAB7DA62C7A5C73FACE5FFBA2F1DD80
A29ADC43399CFCA22279B89A264810E5B926BB5E0D3F727A763E16013F89F8FEAC59
D0FBDD5E8B0C52827E5490F13B84C3634E89C6D1731AE5F1A60F88ED118D080E1AB2
CAA532D06C2F7D2A0874DEE4E6B6E57283F6478DAF4253DB45010000000120588076
CEFA5BCC5D76A66043EDAAC2E4BFBA513CE4AE07079564144BF207F4698531616705
2394A083F7B69FD35BFBED043AD8B2628288DD2F8E19C86C20C7DEE2B69AFA091B82
EFABDBC5ABBD9F91C8459D14FF8CFBF6D10F68EA5FAFAE7474988210D829AF1BC67E01
A5DFEA430AAA07242A886D4307014EDF6C1A42E02D0B893521
```

Annotated hex:

- * See the annotated hex for the C509 type 2 certificate in Section 3.2.4. The only differences are the certificate type, the signature value, and the key identifiers.

3.2.4. C509 Type 2 Certificate

Plain hex (297 bytes):

```
024212341818F61A6775D7001A69570A80D830481234567890ABCDEF00825880B809
2F6F04726A921CFAB2D313AE9D2F01C7CE465FAB7DA62C7A5C73FACE5FFBA2F1DD80
A29ADC43399CFCA22279B89A264810E5B926BB5E0D3F727A763E16013F89F8FEAC59
D0FBDD5E8B0C52827E5490F13B84C3634E89C6D1731AE5F1A60F88ED118D080E1AB2
CAA532D06C2F7D2A0874DEE4E6B6E57283F6478DAF4253DB45010000000120588050
7EE326549994969B3FAD4309A2704F424E435A24C505603F51104F1E8DDB153D784A
9E34E88BC74F67143970B0FCBD2119AC89E87ABF9C2818FFBF5C6993F87F7A5B640B
B7E0FDBCE5F2136377F70C279D76866D725E5868F4FE56F031E80ACBEDE58A6E1AD1
CD65A0ADB303C555F408651D5E7F752805EA4B79EF36105344
```

Annotated hex:

```

0: 02          # [0]. certificate type=2
1: 42          # [1]. certificateSerialNumber=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     # modulus=byte[128]
32:   B8092F6F04726A921CFAB2D313AE9D2F01C7CE465FAB7DA62C7A5C73FA
61:   CE5FFBA2F1DD80A29ADC43399CFCA22279B89A264810E5B926BB5E0D3F
90:   727A763E16013F89F8FEAC59D0FBDD5E8B0C52827E5490F13B84C3634E
119:  89C6D1731AE5F1A60F88ED118D080E1AB2CAA532D06C2F7D2A0874DEE4
148:  E6B6E57283F6478DAF4253DB
160:  45        # exponent=byte[5]
161:  0100000001
166: 20        # [9]. extensions=-1, KeyUsage, critical:
                #      [digitalSignature]
167: 58 80     # [10]. signature value=byte[128]
169:  507EE326549994969B3FAD4309A2704F424E435A24C505603F51104F1E8D
199:  DB153D784A9E34E88BC74F67143970B0FCBD2119AC89E87ABF9C2818FFBF
229:  5C6993F87F7A5B640BB7E0FDBCE5F2136377F70C279D76866D725E5868F4
259:  FE56F031E80ACBEDE58A6E1AD1CD65A0ADB303C555F408651D5E7F752805
289:  EA4B79EF36105344

```

3.3. Weierstrass EC Public Key On Curve secp256r1

- * Self-signed certificate
- * EC public key on the curve secp256r1
- * Signature algorithm: ecdsa-with-sha256
- * Subject: a commonName containing an even number of lowercase hexadecimal characters
- * Extensions
 - Basic Constraints: CA, without pathLenConstraint
 - Extended Key Usage: only an integer-identified usage
 - Subject Key Identifier

3.3.1. Private Key

```
-----BEGIN PRIVATE KEY-----
MEECAQAwEwYHKoZiZj0CAQYIKoZiZj0DAQcEJzAlAgEBBcAMGYOct/eLyZgLXgeP
Q3jT81GUERXqvBvkzaxRDlpG7A==
-----END PRIVATE KEY-----
```

3.3.2. X.509 Certificate

PEM content (383 bytes):

```
-----BEGIN CERTIFICATE-----
MIIBezCCASCgAwIBAgICEjQwCgYIKoZiZj0EAWIwGzEZMBcGA1UEAwQMTIzNDU2
Nzg5MGFiY2RlZjAeFw0yNTAxMDIwMDAwMDBaFw0yNjAxMDIwMDAwMDBaMBsxGTAX
BgNVBAMMEDEyMzQ1OTBhYmNkZWYwWTATBgqhkhjOPQIBBggqhkhjOPQMBBwNC
AAT0E1lqhXJZlbtg2Le++8TW7bEfYa8IqzJAjU/5+QeN26s2Na/UltVlaiLv3D1Z
xEgqmYNrslj79Mp405MENshXo1QwUjAdBgNVHQ4EFgQUB+EsTKzpXCKF7EpbBaSi
uw7IenowCwYDVR0PBAQDAgEGMA8GA1UdEwEB/wQFMAMBAf8wEwYDVR0lBAwwCgYI
KwYBBQUHAWEwCgYIKoZiZj0EAWIDSQAwwRgIhAIol6Kq7pLGbjg0VlqR2wsQvUGj1
80V2BoBuLyhKIubnAiEAp5m4CfQ2QkbnOJOzzBDOKLXtmsX+4pVCSDuF5iQ7wT8=
-----END CERTIFICATE-----
```

Textual Representation:

Certificate:

Version: v3 (2)

Serial Number:

12:34

Issuer: CN=1234567890abcdef

Validity:

Not Before: Thu Jan 02 01:00:00 CET 2025

Not After : Fri Jan 02 01:00:00 CET 2026

Subject: CN=1234567890abcdef

Subject Public Key Info:

Public Key Algorithm: EC/P256

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 subjectKeyIdentifier:

07:e1:2c:4c:ac:e9:5c:22:85:ec:4a:5b:05:a4:a2:bb:0e:c8:7a:7a

X509v3 keyUsage:

keyCertSign, cRLSign

X509v3 basicConstraints: critical

CA: true, pathlen: null

X509v3 extendedKeyUsage:

kp-serverAuth

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:a7:99:b8:09:f4:36:42:46:e7:a0:93:b3:cc:10:

ce:28:b5:ed:9a:c5:fe:e2:95:42:48:3b:85:e6:24:3b:c1:3f

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
5C2285EC4A5B05A4A2BB0EC87A7A0218602320080158408A25E8AABBA4B19B8E0D15
96A476C2C42F5068F5F3457606806E2F284A22E6E7A799B809F4364246E7A093B3CC
10CE28B5ED9AC5FEE29542483B85E6243BC13F
```

Annotated hex:

- * See the annotated hex for the C509 type 2 certificate in Section 3.3.4. The only differences are the certificate type, the signature value, and the public key identifier.

3.3.4. 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]. certificateSerialNumber=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 on
                #       curve secp256r1
26: 58 41       # [8]. subject public key=EC point=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. Compressed Weierstrass EC Public Key On Curve secp256r1

- * Self-signed certificate
- * EC public key on the curve secp256r1, compressed only in the C509 certificates
- * Signature algorithm: ecdsa-with-sha256
- * Subject: a commonName containing an even number of lowercase hexadecimal characters

* Extensions

- Basic Constraints: CA, without pathLenConstraint
- Extended Key Usage: only an integer-identified usage
- Subject Key Identifier

3.4.1. Private Key

See Section 3.3.1

3.4.2. X.509 Certificate

PEM content (383 bytes):

```
-----BEGIN CERTIFICATE-----
MIIBezCCASCgAwIBAgICEjQwCgYIKoZIzj0EAwIwGzEZMBcGA1UEAwQMTIzNDU2
Nzg5MGFiY2RlZjAeFw0yNTAxMDIwMDAwMDBaFw0yNjAxMDIwMDAwMDBaMBsxGTAX
BgNVBAMMEDEyMzQ1Njc4OTBhYmNkZWYwWTATBgqhkhjOPQIBBggqhkhjOPQMBBwNC
AAT0E1lqhXJZlbtG2Le++8TW7bEfYa8IqzJAjU/5+QeN26s2Na/UltVlaiLv3D1Z
xEgqmYNrslj79Mp405MENshXo1QwUjAdBgNVHQ4EFgQUB+EsTKzpXCKF7EpbBaSi
uw7IenowCwYDVR0PBAQDAgEGMA8GA1UdEwEB/wQFMAMBAf8wEwYDVR0lBAwwCgYI
KwYBBQUHAWewCgYIKoZIzj0EAwIDSQAwwRgIhAIol6Kq7pLGbjg0VlqR2wsQvUGj1
80V2BoBuLyhKIubnAiEAp5m4CfQ2QkbnoJOzzBDOKLXtmsX+4pVCSDuF5iQ7wT8=
-----END CERTIFICATE-----
```

Textual Representation:

Certificate:

Version: v3 (2)

Serial Number:

12:34

Issuer: CN=1234567890abcdef

Validity:

Not Before: Thu Jan 02 01:00:00 CET 2025

Not After : Fri Jan 02 01:00:00 CET 2026

Subject: CN=1234567890abcdef

Subject Public Key Info:

Public Key Algorithm: EC/P256

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 subjectKeyIdentifier:

07:e1:2c:4c:ac:e9:5c:22:85:ec:4a:5b:05:a4:a2:bb:0e:c8:7a:7a

X509v3 keyUsage:

keyCertSign, cRLSign

X509v3 basicConstraints: critical

CA: true, pathlen: null

X509v3 extendedKeyUsage:

kp-serverAuth

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:a7:99:b8:09:f4:36:42:46:e7:a0:93:b3:cc:10:

ce:28:b5:ed:9a:c5:fe:e2:95:42:48:3b:85:e6:24:3b:c1:3f

3.4.3. C509 Type 3 Certificate

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

Plain hex (157 bytes):

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

Annotated hex:

- * See the annotated hex for the C509 type 2 certificate in Section 3.4.4. The only differences are the certificate type, the signature value, and the public key identifier.

3.4.4. C509 Type 2 Certificate

Plain hex (157 bytes):

```
0242123400F61A6775D7001A69570A80481234567890ABCDEF015821FDF413596A87
125995B4E0D8B7BEFBC4D6EDB11F61AF08AB32408D4FF9F9078DDB88015426CD540B
3E3D99A64AAB0B62ECA277B4359EAD040218602320080158408A25E8AABBA4B19B8E
0D1596A476C2C42F5068F5F3457606806E2F284A22E6E7017CEE1E3B865C5EEA2A79
46503C5BA1C39424F71ACDC6AFA5FB55F7E397B83C
```

Annotated hex:

```

0: 02          # [0]. certificate type=2
1: 42          # [1]. certificateSerialNumber=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 on
                #      curve secp256r1
26: 58 21       # [8]. subject public key=EC point=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:  26CD540B3E3D99A64AAB0B62ECA277B4359EAD04
                # 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: E6E7017CEE1E3B865C5EEA2A7946503C5BA1C39424F71ACDC6AFA5FB55F7
153: E397B83C

```

3.5. Weierstrass EC Public Key On Curve secp384r1

- * Self-signed certificate
- * EC public key on the curve secp384r1
- * Subject: a commonName containing free-form text
- * Extensions
 - Basic Constraints: CA, with pathLenConstraint
 - Extended Key Usage: only an OID-identified usage

- Certificate Policies
- Inhibit anyPolicy

3.5.1. Private Key

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

3.5.2. X.509 Certificate

PEM content (539 bytes):

```
-----BEGIN CERTIFICATE-----
MIICFzCCAZ6gAwIBAgICEjQwCgYIKoZIzj0EAwMwHTEbMBkGA1UEAwSc2VsZnNp
Z24tc2VjcDM4NHlxMB4XDTE1MDEwMjAwMDAwMFoXDTE1MDEwMjAwMDAwMFowHTEb
MBkGA1UEAwSc2VsZnNpZ24tc2VjcDM4NHlxMHYwEAYHKoZIzj0CAQYFK4EEACID
YgAE3Wdi8DWJlFE3Ky/ptSqDFK0Q4sQ2PFpYSeKW/lGqub/QOrA40zQYoLzYMoCr
oL2RBAFzZcBItTRrVBCeRj/MiJ5O6HC1+KLGP5BTeGXVb4nihdeBA1KTBo05G6S
Slwpo4GwMIGtMASGA1UdDwQEAwIBBjASBgNVHRMBAf8ECDAGAQH/AgEBMGgGA1Ud
IARhMF8wCAYGZ4EMAQIDMFMBFUdIAAwSzAiBggrBgEFBQcCARYWahr0cDovL2Nw
cy5leGFtcGxlLnNvbTAlBggrBgEFBQcCAjAZDBd0aGlzIGlzIHRobzSB1c2VyIG5v
dGJjZTAUBgNVHSUEDTALBgkrBgEEAYH9WQQwCgYDVz02BAMCAQAwCgYIKoZIzj0E
AwMDZwAwZAIwNH617Unh9lNuKj87XfHBLZuu9EDfveK9RdMfSz/avfqdaFqEWC2Y
sbJHqhDxx4XaAjA0gnN1wF0oDGkz6hPat63ExIwGXALM0hnZAIyqqLHtv6b3oa56
KppqhQZ6RL8aIe8=
-----END CERTIFICATE-----
```

Textual Representation:

Certificate:

Version: v3 (2)

Serial Number:

12:34

Issuer: CN=selfsign-secp384r1

Validity:

Not Before: Thu Jan 02 01:00:00 CET 2025

Not After : Fri Jan 02 01:00:00 CET 2026

Subject: CN=selfsign-secp384r1

Subject Public Key Info:

Public Key Algorithm: EC/P384

Pub:

04:dd:67:62:f0:35:89:94:51:37:2b:2f:e9:b5:2a:83:14:ad:

10:e2:c4:36:3c:5a:58:49:e2:96:fe:51:aa:b9:bf:d0:3a:b0:

38:d3:34:18:a0:bc:d8:32:80:ab:a0:bd:91:04:01:71:65:c0:

48:b5:34:6b:54:10:9e:44:9f:cc:88:9e:4e:e8:70:b5:f8:a2:

c6:3d:ae:41:4d:e1:97:55:be:27:8a:17:5e:04:0d:4a:4c:1a:

0e:e4:6e:92:4a:5c:29

X509v3 extensions:

X509v3 keyUsage:

keyCertSign, cRLSign

X509v3 basicConstraints: critical

CA: true, pathlen: 1

X509v3 certificatePolicies:

Policy: Individual Validation (IV)

Policy: Any Policy

CPS: http://cps.example.com

User Notice: [this is the user notice]

X509v3 extendedKeyUsage:

1.3.6.1.4.1.32473.4

X509v3 inhibitAnyPolicy:

02:01:00

Signature Algorithm: SHA384WITHECDSA

Signature Value:

30:64:02:30:34:7e:b5:ed:49:e1:f6:53:6e:2a:3f:3b:5d:f1:

c1:2d:9b:ae:f4:40:df:bc:42:bd:45:d3:1f:4b:3f:da:bd:fa:

9d:68:5a:84:58:2d:98:b1:b2:47:42:10:f1:c7:85:da:02:30:

34:82:73:75:c0:5d:28:0c:69:33:ea:13:da:b7:ad:c4:c4:8c:

06:5c:02:cc:d2:19:d9:00:8c:aa:a8:b1:ed:bf:a6:f7:a1:ae:

7a:2a:9a:6a:85:06:7a:44:bf:1a:21:ef

3.5.3. C509 Type 3 Certificate

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

Plain hex (308 bytes):

```

0342123401F61A6775D7001A69570A807273656C667369676E2D7365637033383472
3102586104DD6762F035899451372B2FE9B52A8314AD10E2C4363C5A5849E296FE51
AAB9BFD03AB038D33418A0BCD83280ABA0BD9104017165C048B5346B54109E449FCC
889E4EE870B5F8A2C63DAE414DE19755BE278A175E040D4A4C1A0EE46E924A5C298A
02186023010684038000840176687474703A2F2F6370732E6578616D706C652E636F
6D027774686973206973207468652075736572206E6F7469636508492B0601040181
FD5904181E005860347EB5ED49E1F6536E2A3F3B5DF1C12D9BAEF440DFBC42BD45D3
1F4B3FDABDFA9D685A84582D98B1B2474210F1C785DA34827375C05D280C6933EA13
DAB7ADC4C48C065C02CCD219D9008CAA8B1EDBFA6F7A1AE7A2A9A6A85067A44BF1A
21EF

```

Annotated hex:

- * See the annotated hex for the C509 type 2 certificate in Section 3.5.4. The only differences are the certificate type, the signature value, and the key identifiers.

3.5.4. C509 Type 2 Certificate

Plain hex (308 bytes):

```

0242123401F61A6775D7001A69570A807273656C667369676E2D7365637033383472
3102586104DD6762F035899451372B2FE9B52A8314AD10E2C4363C5A5849E296FE51
AAB9BFD03AB038D33418A0BCD83280ABA0BD9104017165C048B5346B54109E449FCC
889E4EE870B5F8A2C63DAE414DE19755BE278A175E040D4A4C1A0EE46E924A5C298A
02186023010684038000840176687474703A2F2F6370732E6578616D706C652E636F
6D027774686973206973207468652075736572206E6F7469636508492B0601040181
FD5904181E005860347EB5ED49E1F6536E2A3F3B5DF1C12D9BAEF440DFBC42BD45D3
1F4B3FDABDFA9D685A84582D98B1B2474210F1C785DA055BE26787AB4DD58FD330E3
435AC84EBE49A4382FB964591C3EACC9A04F3814FC2964C1B4B201C013AE7CCB3727
CDF7

```

Annotated hex:

```

0: 02          # [0]. certificate type=2
1: 42          # [1]. certificateSerialNumber=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 on
                #      curve secp384r1
36: 58 61        # [8]. subject public key=EC point=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: 84 # value=array[4]
      # CertificatePolicy[0]
143: 03 # PolicyIdentifier=3:
      # individual-validated
144: 80 # PolicyQualifierInfos=array[0]
      # CertificatePolicy[1]
145: 00 # PolicyIdentifier=0: anyPolicy
146: 84 # PolicyQualifierInfos=array[4]
      # PolicyQualifierInfo[0]
147: 01 # policyQualifierId=1:
      # domain-validated
148: 76 # qualifier=char[22]
149: 687474703A2F2F6370732E657861 # "http://cps.exe"
163: 6D706C652E636F6D # "mple.com"
      # PolicyQualifierInfo[1]
171: 02 # policyQualifierId=2:
      # organization-validated
172: 77 # qualifier=char[23]
173: 7468697320697320746865207573 # "this is the us"
187: 6572206E6F74696365 # "er notice"
      # extension[3]
196: 08 # type=8: ExtendedKeyUsage
197: 49 # byte[9]:
198: 2B0601040181FD5904 # oid: 1.3.6.1.4.1.32473.4
      # extension[4]
207: 18 1E # type=30: InhibitAnyPolicy
209: 00 # value=simple-uint(0)
210: 58 60 # [10]. signature value=byte[96]
212: 347EB5ED49E1F6536E2A3F3B5DF1C12D9BAEF440DFBC42BD45D31F4B3FDA
242: BDF9A9D685A84582D98B1B2474210F1C785DA055BE26787AB4DD58FD330E3
272: 435AC84EBE49A4382FB964591C3EACC9A04F3814FC2964C1B4B201C013AE
302: 7CCB3727CDF7
```

3.6. Weierstrass EC Public Key On Curve secp521r1

- * Self-signed certificate
- * EC public key on the curve secp521r1
- * Signature algorithm: ecdsa-with-sha512
- * Subject: empty
- * Extensions
 - Basic Constraints: non-CA
 - Extended Key Usage: integer-identified and OID-identified usages
 - Subject Alternative Name

3.6.1. Private Key

```
-----BEGIN PRIVATE KEY-----
MGACAQAwEAYHkoZIZj0CAQYFK4EEACMESTBHAgEBBEIBTyH+UdnGf8eNYO8U2b7w
Z4A21kT4P50ZOUTjpDPxIkovVX2d6SpSsMnlnjLAikYP2YOZwZZwd86lpB1+7sdS
a/Y=
-----END PRIVATE KEY-----
```

3.6.2. X.509 Certificate

PEM content (753 bytes):


```
RegisteredID: 1.3.6.1.4.1.32473.8
IP: 17.17.17.17
OtherName: 1.3.6.1.4.1.32473.1 = h'22222222222222222222'
OtherName: MACAddress:22-22-22-22-22-22
OtherName: Smtputf8Mailbox:smtputf8mailbox@example.com
OtherName: hardwareModuleName:1.3.6.1.4.1.32473.2 =
    h'0410333333333333333333333333333333333333'
X509v3 basicConstraints: critical
    CA: false
X509v3 extendedKeyUsage:
    kp-clientAuth
    kp-serverAuth
Signature Algorithm: SHA512WITHECDSA
Signature Value:
30:81:88:02:42:01:2f:83:58:f6:46:21:ca:68:f7:db:64:4a:
ef:e3:79:58:04:1a:68:64:36:af:ce:dd:e7:0a:ce:ba:73:74:
4d:70:14:77:84:a4:1a:d6:76:73:a1:ee:5b:3b:9b:1a:83:51:
55:3a:29:e8:78:15:ab:fc:ca:5d:1d:e1:09:9f:28:4b:4c:02:
42:01:b7:db:35:73:cf:f7:c9:75:99:70:5e:fa:41:9f:98:2d:
66:28:7a:44:41:77:73:36:a4:2b:e9:b8:b3:a7:fb:57:d0:34:
85:44:24:4b:ee:9b:ae:21:7d:ac:7a:7d:80:77:1d:c6:8a:ba:
bd:57:27:70:40:40:3c:fd:bb:84:06:86:eb:68
```

3.6.3. C509 Type 3 Certificate

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

Plain hex (512 bytes):

0342123402F61A6775D7001A69570A808003588504005538CE8F7CDE229335C85958
AACD029DDF65CFC2A72A75055E63B8FE59D07FB4BDF10DB7B8BA7D57C5C691EB96EA
B97411615A6A430E51787031719CEBC305E69200705CC828B9755F8FD53452B777A4
0CB6792554E5718BAB91EA3F03086A4072A47047CEEC2493C384045FCC6ED8E4F748
A5223AF12901EB2E19A6C288951C939B05880201039604840462444501676578616D
706C65026F6162632E6578616D706C652E636F6D016F616263406578616D706C652E
636F6D2174736D747075746638406578616D706C652E636F6D06781C687474703A2F
2F6D797572692E6578616D706C652E636F6D2F61626308492B0601040181FD590807
44111111110082492B0601040181FD59014C040A22222222222222222222222222222222
2222222221781C736D74702E757466386D61696C626F78406578616D706C652E636F
6D2082492B0601040181FD59025204103321
088202015884012F8358F64621CA68F7DB644AEFE37958041A686436AFCEDE70ACE
BA73744D70147784A41AD67673A1EE5B3B9B1A8351553A29E87815ABFCCA5D1DE109
9F284B4C01B7DB3573CFF7C97599705EFA419F982D66287A4441777336A42BE9B8B3
AFB57D0348544244BEE9BAE217DAC7A7D80771DC68ABABD572770403CFDBB840686
E768

Annotated hex:

- * See the annotated hex for the C509 type 2 certificate in Section 3.6.4. The only differences are the certificate type, the signature value, and the key identifiers.

3.6.4. C509 Type 2 Certificate

Plain hex (512 bytes):

```
0242123402F61A6775D7001A69570A808003588504005538CE8F7CDE229335C85958
AACD029DDF65CFC2A72A75055E63B8FE59D07FB4BDF10DB7B8BA7D57C5C691EB96EA
B97411615A6A430E51787031719CEBC305E69200705CC828B9755F8FD53452B777A4
0CB6792554E5718BAB91EA3F03086A4072A47047CEEC2493C384045FCC6ED8E4F748
A5223AF12901EB2E19A6C288951C939B05880201039604840462444501676578616D
706C65026F6162632E6578616D706C652E636F6D016F616263406578616D706C652E
636F6D2174736D747075746638406578616D706C652E636F6D06781C687474703A2F
2F6D797572692E6578616D706C652E636F6D2F61626308492B0601040181FD590807
44111111110082492B0601040181FD59014C040A22222222222222222222222222222222
2222222221781C736D74702E757466386D61696C626F78406578616D706C652E636F
6D2082492B0601040181FD59025204103333333333333333333333333333333333333
088202015884012F8358F64621CA68F7DB644AEFE37958041A686436AFCEDDE70ACE
BA73744D70147784A41AD67673A1EE5B3B9B1A8351553A29E87815ABFCCA5D1DE109
9F284B4C00ED9B37F0DA14D5086C5E3195C84346364CBB9CB0B2E36FFADDE2A8D170
A7B92F4F4C0AEB15CAC4F71968E2A5A04A17FBF3BCDC45B5286C491FE10F6CD53A26
413F
```

Annotated hex:

```
0: 02          # [0]. certificate type=2
1: 42          # [1]. certificateSerialNumber=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 on
          #      curve secp521r1
18: 58 85       # [8]. subject public key=EC point=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:      96      # value=array[22]
                  # 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:      67      # value=char[7]
166:      6578616D706C65 # "example"
                  # GeneralName[1]
173:      02      # GeneralNameType=2: dNSName
174:      6F      # GeneralNameValue=char[15]
175:      6162632E6578616D706C652E636F6D # "abc.example.com"
                  # GeneralName[2]
190:      01      # GeneralNameType=1: rfc822Name
191:      6F      # GeneralNameValue=char[15]
192:      616263406578616D706C652E636F6D # "abc@example.com"
                  # GeneralName[3]
207:      21      # GeneralNameType=-2: on-SmtpUTF8Mailbox
208:      74      # GeneralNameValue=char[20]
209:      736D747075746638406578616D706C # "smtputf8@exampl"
224:      652E636F6D # "e.com"
                  # GeneralName[4]
229:      06      # GeneralNameType=6: uri
230:      78 1C     # GeneralNameValue=char[28]
232:      687474703A2F2F6D797572692E6578 # "http://myuri.ex"
247:      616D706C652E636F6D2F616263     # "ample.com/abc"
                  # GeneralName[5]
260:      08      # GeneralNameType=8: registeredID
261:      49      # GeneralNameValue=byte[9]:
262:      2B0601040181FD5908 # oid: 1.3.6.1.4.1.32473.8
                  # GeneralName[6]
271:      07      # GeneralNameType=7: ipAddress
272:      44      # GeneralNameValue=byte[4]
273:      11111111
                  # GeneralName[7]
277:      00      # GeneralNameType=0: otherName
278:      82      # GeneralNameValue=array[2]
279:      49      # id=byte[9]:
280:      2B0601040181FD5901 # oid: 1.3.6.1.4.1.32473.1
289:      4C      # value=byte[12]
290:      040A222222222222222222222222
```

```

# GeneralName[8]
302:      22          # GeneralNameType=-3: on-MACAddress
303:      46          # GeneralNameValue=byte[6]
304:      222222222222
                        # GeneralName[9]
310:      21          # GeneralNameType=-2: on-SmtpUTF8Mailbox
311:      78 1C        # GeneralNameValue=char[28]
313:      736D74702E757466386D61696C626F # "smtp.utf8mailbo"
328:      78406578616D706C652E636F6D     # "x@example.com"
                        # GeneralName[10]
341:      20          # GeneralNameType=-1:
                        # on-hardwareModuleName
342:      82          # GeneralNameValue=array[2]
343:      49          # id=byte[9]:
344:      2B0601040181FD5902 # oid: 1.3.6.1.4.1.32473.2
353:      52          # value=byte[18]
354:      041033333333333333333333333333333333
                        # extension[2]
372:      23          # type=-4: BasicConstraints, critical
373:      21          # value=-2: CA: false
                        # extension[3]
374:      08          # type=8: ExtendedKeyUsage
375:      82          # value=array[2]
376:      02          # 2: clientAuth
377:      01          # 1: serverAuth
378: 58 84           # [10]. signature value=byte[132]
380:      012F8358F64621CA68F7DB644AEFE37958041A686436AFCEDE70ACEBA73
410:      744D70147784A41AD67673A1EE5B3B9B1A8351553A29E87815ABFCCA5D1D
440:      E1099F284B4C00ED9B37F0DA14D5086C5E3195C84346364CBB9CB0B2E36F
470:      FADDE2A8D170A7B92F4FC0AEB15CAC4F71968E2A5A04A17FBFB3BCDC45B5
500:      286C491FE10F6CD53A26413F

```

3.7. Weierstrass EC Public Key On Curve sm2p256v1

- ```
* Self-signed certificate
* EC public key on the curve sm2p256v1
* Signature algorithm: sm2-with-sm3
* Subject:
 - serialNumber
 - organization
 - organizationalUnit
```

- organizationIdentifier

- \* Extensions:

- Policy Constraints containing only inhibitPolicyMapping
- Name Constraints containing only excludedSubTrees

### 3.7.1. Private Key

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

### 3.7.2. X.509 Certificate

PEM content (644 bytes):

```
-----BEGIN CERTIFICATE-----
MIICGDCCAiagAwIBAgICEjQwCgYIKoEcz1UBg3UwgZUxGzAZBgNVBAMMENlbGZz
aWduLXNtMnAyNTZ2MTEYMBYGA1UEBQwPbXkgc2VyaWFsTnVtYmVyMRgwFgYDVQK
DA9teSBvcmdhbml6YXRpb24xHjAcBgNVBAsMFw15IG9yZ2FuaXphdGlvbmFsVW5p
dDEiMCAGA1UEYQwZbXkgb3JnYW5pemF0aW9uSWRlbnRpZml1c jAeFw0yNTAxMDIw
MDAwMDBaFw0yNjAxMDIwMDAwMDBaMIGVMRswGQYDVQQDDBJzZWxmc2lnbi1zbTJw
MjU2d jExGDAWBgNVBAUMD215IHNLcm1hbmE51bWJlc jEYMBYGA1UECgwPbXkgb3Jn
YW5pemF0aW9uMR4wHAYDVQQLDBVteSBvcmdhbml6YXRpb25hbFVuaXQxI jAgBgNV
BGEMGW15IG9yZ2FuaXphdGlvbk1kZW50aWZpZXIwWTATBgqhkJOPQIBBggqgRzP
VQGCLQNCASV//S+hhHIFJyBrewUEl2synRqLz/ j jNLqtxHoyZ8QH7tEhCPxZvn/
2Y8OMhWXuzlINab7JAM3o4kSkHoiw/BKo2QwY jALBgNVHQ8EBAMCB4AwRQYDVR0e
BD4wPKE6MBuCGWV4Y2x1ZGVkLmRucEuZXhhbXBsZS5jb20wG4IZZXhjbHVkZWQu
ZG5zMi5leGftcGx1LmNvbTAMBgNVHSQEETADgQECMAoGCCqBHM9VAYN1A0gAMEUC
IFqV641WbBysLPl+0sfFD+L8eG4Zb56Ry3DVP1O3VGiQAiEAjCVf7QY1cbj6AOqX
T+yb/N3maosc9h6BcL00XD/QZ7Y=
-----END CERTIFICATE-----
```

Textual Representation:

## Certificate:

Version: v3 (2)

Serial Number:

12:34

Issuer: CN=selfsign-sm2p256v1,SERIALNUMBER=my serialNumber,O=my organization,OU=my organizationalUnit,organizationIdentifier=my organizationIdentifier

## Validity:

Not Before: Thu Jan 02 01:00:00 CET 2025

Not After : Fri Jan 02 01:00:00 CET 2026

Subject: CN=selfsign-sm2p256v1,SERIALNUMBER=my serialNumber,O=my organization,OU=my organizationalUnit,organizationIdentifier=my organizationIdentifier

## Subject Public Key Info:

Public Key Algorithm: EC/SM2

Pub:

04:95:ff:f4:be:86:11:c8:14:9c:81:ad:ec:14:12:5d:ac:ca:  
74:6a:2f:3f:e3:8c:d2:ea:b7:11:e8:c9:9f:10:1f:bb:44:84:  
23:f1:66:f9:ff:d9:8f:0e:32:15:97:bb:39:48:35:a6:fb:24:  
03:37:a3:89:12:90:7a:22:c3:f0:4a

## X509v3 extensions:

X509v3 keyUsage:

digitalSignature

X509v3 nameConstraints:

Excluded

DNS: excluded.dns1.example.com

DNS: excluded.dns2.example.com

X509v3 policyConstraints:

Require Explicit Policy:null, Inhibit Explicit Policy:2

Signature Algorithm: SM3WITHSM2

Signature Value:

30:45:02:20:5a:95:eb:8d:56:6c:1c:ac:2c:f9:7e:d2:c7:c5:  
0f:e2:fc:78:6e:19:6f:9e:91:cb:70:d5:3e:53:b7:54:68:90:  
02:21:00:8c:25:5f:ed:06:35:71:b8:fa:00:ea:97:4f:ec:9b:  
fc:dd:e6:6a:8b:1c:f6:1e:81:70:bd:34:5c:3f:d0:67:b6

## 3.7.3. C509 Type 3 Certificate

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

Plain hex (325 bytes):

```

0342123408F61A6775D7001A69570A808A017273656C667369676E2D736D32703235
367631036F6D792073657269616C4E756D626572086F6D79206F7267616E697A6174
696F6E09756D79206F7267616E697A6174696F6E616C556E69741278196D79206F72
67616E697A6174696F6E4964656E7469666965720658410495FFF4BE8611C8149C81
ADEC14125DACC746A2F3FE38CD2EAB711E8C99F101FBB448423F166F9FFD98F0E32
1597BB394835A6FB240337A38912907A22C3F04A860201181A82F684027819657863
6C756465642E646E73312E6578616D706C652E636F6D0278196578636C756465642E
646E73322E6578616D706C652E636F6D181C82F60258405A95EB8D566C1CAC2CF97E
D2C7C50FE2FC786E196F9E91CB70D53E53B75468908C255FED063571B8FA00EA974F
EC9BFCDD66A8B1CF61E8170BD345C3FD067B6

```

Annotated hex:

- \* See the annotated hex for the C509 type 2 certificate in Section 3.7.4. The only differences are the certificate type, the signature value, and the key identifiers.

### 3.7.4. C509 Type 2 Certificate

Plain hex (325 bytes):

```

0242123408F61A6775D7001A69570A808A017273656C667369676E2D736D32703235
367631036F6D792073657269616C4E756D626572086F6D79206F7267616E697A6174
696F6E09756D79206F7267616E697A6174696F6E616C556E69741278196D79206F72
67616E697A6174696F6E4964656E7469666965720658410495FFF4BE8611C8149C81
ADEC14125DACC746A2F3FE38CD2EAB711E8C99F101FBB448423F166F9FFD98F0E32
1597BB394835A6FB240337A38912907A22C3F04A860201181A82F684027819657863
6C756465642E646E73312E6578616D706C652E636F6D0278196578636C756465642E
646E73322E6578616D706C652E636F6D181C82F602584059F40C77AE8AC0BD0638E0
B822001FD47EEF15667C7034436A95C97E94CEEE5FEFA1441C1F6537A76692605BED
70A1168D2AFE6B03B4E9F925024D1B76729555

```

Annotated hex:

```

0: 02 # [0]. certificate type=2
1: 42 # [1]. certificateSerialNumber=byte[2]
2: 1234
4: 08 # [2]. signature alg=8: sm2-with-sm3
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: 72 # value=char[18]
19: 73656C667369676E2D736D3270323536 # "selfsign-sm2p256"
35: 7631 # "v1"

```

```

attribute[1]
37: 03 # type=3: serialNumber
38: 6F # value=char[15]
39: 6D792073657269616C4E756D626572 # "my serialNumber"
attribute[2]
54: 08 # type=8: organization
55: 6F # value=char[15]
56: 6D79206F7267616E697A6174696F6E # "my organization"
attribute[3]
71: 09 # type=9: organizationalUnit
72: 75 # value=char[21]
73: 6D79206F7267616E697A6174696F6E61 # "my organizationa"
89: 6C556E6974 # "lUnit"
attribute[4]
94: 12 # type=18: organizationIdentifier
95: 78 19 # value=char[25]
97: 6D79206F7267616E697A6174696F6E49 # "my organizationI"
113: 64656E746966696572 # "dentifier"
122: 06 # [7]. subjectPublicKeyAlg=6: EC public key on
curve sm2p256v1
123: 58 41 # [8]. subject public key=EC point=byte[65]
125: 0495FFF4BE8611C8149C81ADEC14125Dacca746A2F3FE38CD2EAB711E8C9
155: 9F101FBB448423F166F9FFD98F0E321597BB394835A6FB240337A3891290
185: 7A22C3F04A
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: F6 # permittedSubtrees=<null>
197: 84 # excludedSubtrees=array[4]
GeneralName[0]
198: 02 # GeneralNameType=2: dNSName
199: 78 19 # GeneralNameValue=char[25]
201: 6578636C756465642E646E73312E65 # "excluded.dns1.e"
216: 78616D706C652E636F6D # "xample.com"
GeneralName[1]
226: 02 # GeneralNameType=2: dNSName
227: 78 19 # GeneralNameValue=char[25]
229: 6578636C756465642E646E73322E65 # "excluded.dns2.e"
244: 78616D706C652E636F6D # "xample.com"
extension[2]
254: 18 1C # type=28: PolicyConstraints
256: 82 # value=array[2]
257: F6 # requireExplicitPolicy=<null>
258: 02 # inhibitPolicyMapping=2
```

```
259: 58 40 # [10]. signature value=byte[64]
261: 59F40C77AE8AC0BD0638E0B822001FD47EEF15667C7034436A95C97E94CE
291: EE5FEFA1441C1F6537A76692605BED70A1168D2AFE6B03B4E9F925024D1B
321: 76729555
```

### 3.8. Weierstrass EC Public Key On Curve brainpoolP256r1

- \* Self-signed certificate
- \* EC public key on the curve brainpoolP256r1
- \* Signature algorithm: ecdsa-with-shake128
- \* Subject:
  - country
  - state
  - locality
  - postalCode
  - street
- \* Extensions:
  - IPAddressBlocks with SAFI = null and IP Address Choice = null
  - IPAddressBlocks V2 with SAFI = null and IP Address Choice = null
  - ASIdentifiers
  - ASIdentifiers V2

#### 3.8.1. Private Key

```
-----BEGIN PRIVATE KEY-----
MEICAQAwFAYHKOZizj0CAQYJKyQDAwIIAQEHBCcwJQIBAQQgiOJE752KYXs1GZ0/
+ETWNoBn8L7ZF09gjcd/xtLR/iE=
-----END PRIVATE KEY-----
```

#### 3.8.2. X.509 Certificate

PEM content (646 bytes):

-----BEGIN CERTIFICATE-----

MIICGjCCAimgAwIBAgICEjQwCgYIKwYBBQUHBIAwgYUxITAfBgNVBAMMGHNlbGZzaWduLWJyYWlucG9vbHAYNTZyMTELMakGA1UEBgwCREUxFDASBgNVBACMC215IGxvY2FsaXR5MREwDwYDVQQIDAhteSBzdGF0ZTESMBAGA1UECQwJbXkge3RyZWV0MRYwFAYDVQQRDA1teSBwb3N0YWxDb2RlMB4XDTI1MDEwMjAwMDAwMFoXDTI1MDEwMjAwMDAwMFowYUxITAfBgNVBAMMGHNlbGZzaWduLWJyYWlucG9vbHAYNTZyMTELMakGA1UEBgwCREUxFDASBgNVBACMC215IGxvY2FsaXR5MREwDwYDVQQIDAhteSBzdGF0ZTESMBAGA1UECQwJbXkge3RyZWV0MRYwFAYDVQQRDA1teSBwb3N0YWxDb2RlMFowFAYHkoZiZj0CAQYJKYQDAwIIAQEHA0IABHewd0Eu6YlQd57Ygv/LFkjgFCcjVEaWJPW84vFPMkKtSsxWhqhlCNWftyn9wpgRGI2L8BbOSlFRBU2viIxIle2jgYUwgYIwCwYDVR0PBAQDAGEAMB4GCCsGAQUFBwEHBBIwEDAGBAIAAQUMAYEAgACBQAwhQYIKwYBBQUHAQgEETAPoA0wCwIBAjAGAgEDAgEGMCAGCCsGAQUFBwEcbBQwEjAHBAMAQEFADAHBAMAAgEFADASBggrBgEFBQcBHQQGMASgAgUAMAOGCCsGAQUFBwYgA0cAMEQCIHggH5kJkQjKOqxZN3kK/9+Bzvb10b5iKf4mgvft08NGAiBii7S11hSG8Cbc2q19KPBwN4m/jhwMIHGfXzJC/d7/bQ==

-----END CERTIFICATE-----

Textual Representation:

## Certificate:

Version: v3 (2)

Serial Number:

12:34

Issuer: CN=selfsign-brainpoolp256r1,C=DE,L=my locality,ST=my state,  
STREET=my street,PostalCode=my postalCode

## Validity:

Not Before: Thu Jan 02 01:00:00 CET 2025

Not After : Fri Jan 02 01:00:00 CET 2026

Subject: CN=selfsign-brainpoolp256r1,C=DE,L=my locality,ST=my state  
,STREET=my street,PostalCode=my postalCode

## Subject Public Key Info:

Public Key Algorithm: EC/BRAINPOOLP256R1

Pub:

04:77:b0:77:41:2e:e9:89:50:77:9e:d8:82:ff:cb:16:48:e0:

14:27:23:54:46:96:24:f5:bc:e2:f1:4f:32:42:ad:4a:cc:56:

86:a8:65:08:d5:9f:b7:29:fd:c2:98:11:18:8d:8b:f0:16:ce:

4a:51:51:05:4d:af:88:8c:48:d5:ed

## X509v3 extensions:

X509v3 keyUsage:

digitalSignature

X509v3 sbgp-ipAddrBlock:

IPv4: inherit

IPv6: inherit

X509v3 sbgp-autonomousSysNum:

Autonomous System Numbers:

2

3-6

X509v3 sbgp-ipAddrBlockV2:

IPv4 unicast: inherit

IPv6 unicast: inherit

X509v3 sbgp-autonomousSysNumV2:

Autonomous System Numbers: inherit

Signature Algorithm: SHAKE128WITHECDSA

Signature Value:

30:44:02:20:78:20:1f:99:09:91:08:ca:3a:ac:59:37:79:0a:

ff:df:81:ce:f6:f5:d1:be:62:29:fe:26:82:f7:d3:d3:c3:46:

02:20:62:8b:b4:a5:d6:14:86:f0:26:dc:da:ad:7d:28:f0:70:

37:89:bf:8e:1c:0c:20:71:9f:5f:32:42:fd:de:ff:6d

## 3.8.3. C509 Type 3 Certificate

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

Plain hex (263 bytes):

```

0342123403F61A6775D7001A69570A808C01781873656C667369676E2D627261696E
706F6F6C70323536723104624445056B6D79206C6F63616C69747906686D79207374
61746507696D79207374726565740C6D6D7920706F7374616C436F64651818584104
77B077412EE98950779ED882FFCB1648E014272354469624F5BCE2F14F3242AD4ACC
5686A86508D59FB729FDC29811188D8BF016CE4A5151054DAF888C48D5ED8A020118
208601F6F602F6F6182182028201031822860101F60201F61823F6584078201F9909
9108CA3AAC5937790AFFDF81CEF6F5D1BE6229FE2682F7D3D3C346628BB4A5D61486
F026DCDAAD7D28F0703789BF8E1C0C20719F5F3242FDDEFF6D

```

Annotated hex:

- \* See the annotated hex for the C509 type 2 certificate in Section 3.8.4. The only differences are the certificate type, the signature value, and the key identifiers.

### 3.8.4. C509 Type 2 Certificate

Plain hex (263 bytes):

```

0242123403F61A6775D7001A69570A808C01781873656C667369676E2D627261696E
706F6F6C70323536723104624445056B6D79206C6F63616C69747906686D79207374
61746507696D79207374726565740C6D6D7920706F7374616C436F64651818584104
77B077412EE98950779ED882FFCB1648E014272354469624F5BCE2F14F3242AD4ACC
5686A86508D59FB729FDC29811188D8BF016CE4A5151054DAF888C48D5ED8A020118
208601F6F602F6F6182182028201031822860101F60201F61823F658404BF673AB08
781A572889717416F5B662A188B3218506F1780EB1D17C8B0207FF9F318BB7DBFD17
F6C829E93C0CDCB657E795436FA8FC4240A71F223DC0366059

```

Annotated hex:

```

0: 02 # [0]. certificate type=2
1: 42 # [1]. certificateSerialNumber=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 on
curve brainpoolp256r1
99: 58 41 # [8]. subject public key=EC point=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: IPAddrBlocks
171: 86 # value=array[6]
IPAddrBlock[0]
172: 01 # AFI=1: IPv4
173: F6 # SAFI=<null>
174: F6 # IP Address Choice=<null>
IPAddrBlock[1]
175: 02 # AFI=2: IPv6
176: F6 # SAFI=<null>
177: F6 # IP Address Choice=<null>
extension[2]
178: 18 21 # type=33: ASIdentifiers
180: 82 # value=array[2]
181: 02 # id=2
182: 82 # range=array[2]
183: 01 # min=1
184: 03 # max=3
extension[3]
185: 18 22 # type=34: IPAddrBlocksV2
187: 86 # value=array[6]
IPAddrBlock[0]
```

```

188: 01 # AFI=1: IPv4
189: 01 # SAFI=1: unicast
190: F6 # IP Address Choice=<null>
 # IPAddrBlock[1]
191: 02 # AFI=2: IPv6
192: 01 # SAFI=1: unicast
193: F6 # IP Address Choice=<null>
 # extension[4]
194: 18 23 # type=35: ASIdentifiersV2
196: F6 # value=<null>
197: 58 40 # [10]. signature value=byte[64]
199: 4BF673AB08781A572889717416F5B662A188B3218506F1780EB1D17C8B02
229: 07FF9F318BB7DBFD17F6C829E93C0CDCB657E795436FA8FC4240A71F223D
259: C0366059

```

### 3.9. Weierstrass EC Public Key On Curve brainpoolP384r1

- \* Self-signed certificate
- \* EC public key on the curve brainpoolP384r1
- \* Signature algorithm: ecdsa-with-sha384
- \* Subject:
  - surname
  - givenName
  - title
  - name
- \* Extensions:
  - IPAddrBlocks with non-null SAFI and IntIPAddressChoice'
  - IPAddrBlocks V2 with non-null SAFI, IntIPAddressChoice and IPAddressChoice

#### 3.9.1. Private Key

```

-----BEGIN PRIVATE KEY-----
MFICAQAwFAYHkoZIZj0CAQYJKyQDAwIIAQELBDcwNQIBAQQwgGfwvtKU72CNx3/G
2VH+IU85UqnWjleSVxt87bW/XLcURC4qRMOJB9G6KmsodzwN
-----END PRIVATE KEY-----

```

## 3.9.2. X.509 Certificate

PEM content (717 bytes):

```
-----BEGIN CERTIFICATE-----
MIICyTCCAlCgAwIBAgICEjQwCgYIKoZIzj0EAwMwdDEhMB8GA1UEAwYc2VsZnNp
Z24tYnJhaW5wb29scDM4NHlxMRMwEQYDVQQEDApTeSBzdXJuYW11MREwDwYDVQQM
DAhteSB0aXRszTEVMBMGAlUEKgwMbXkgZ212ZW50YW11MRAwDgYDVQQpDAdteSBu
YW11MB4XDTI1MDEwMjAwMDAwMFoXDTI2MDEwMjAwMDAwMFowdDEhMB8GA1UEAwYc
2VsZnNpZ24tYnJhaW5wb29scDM4NHlxMRMwEQYDVQQEDApTeSBzdXJuYW11MREw
DwYDVQQMDAhteSB0aXRszTEVMBMGAlUEKgwMbXkgZ212ZW50YW11MRAwDgYDVQQp
DAdteSBuYW11MHowFAYHKoZIzj0CAQYJKyQDAwIIAQELA2IABGcJyZKRm0nEj9kx
0FxJfTh15ghMkd86TH54H0GFQ7Aj1Z6L8l0TP7GglOnULI+m7TtG6Yg6NavUsKnT
Cq79m36I7TgAVl0efwYze01lGSktSb1V7DChZxl/7A90KYIrlaOBsDCBrTALBgNV
HQ8EBAMCB4AwSAYIKwYBBQUHAQCEPDA6MBkEAgABMBMBADAAAIDBQTGM2QAAwQA
ywBxMB0EAgACMBcDBwAgAQ24EjQwDAMEAD//BgMEAD//DzBUBggrBgEFBQcBHARI
MEYwGgQDAAEbMBMBADAAAIDBQTGM2QAAwQAYwBxMCgEAgACATAhAwcAIAENuBI0
MBYDBQA//wADAw0AP/8BIgAAIjMzRFVmMAoGCCqGSM49BAMDA2cAMGQCMGcJyZKR
m0nEj9kx0FxJfTh15ghMkd86TH54H0GFQ7Aj1Z6L8l0TP7GglOnULI+m7QIwIO2f
2lowmyyHBN2l8UTxe7MWuYwpEST7pc/sbvl/JogGmubFLis84iMSjdEMKqcw
-----END CERTIFICATE-----
```

Textual Representation:

## Certificate:

Version: v3 (2)

Serial Number:

12:34

Issuer: CN=selfsign-brainpoolp384r1,SURNAME=my surname,T=my title,G  
IVENNAME=my givenName,Name=my name

## Validity:

Not Before: Thu Jan 02 01:00:00 CET 2025

Not After : Fri Jan 02 01:00:00 CET 2026

Subject: CN=selfsign-brainpoolp384r1,SURNAME=my surname,T=my title,  
GIVENNAME=my givenName,Name=my name

## Subject Public Key Info:

Public Key Algorithm: EC/BRAINPOOLP384R1

Pub:

04:67:09:c9:92:91:9b:49:c4:8f:d9:31:d0:5c:49:7d:38:65:  
e6:08:4c:91:df:3a:4c:7e:78:1f:41:85:43:b0:23:d5:9e:8b:  
f2:5d:13:3f:b1:a0:94:e9:d4:2c:8f:a6:ed:3b:46:e9:88:3a:  
35:ab:d4:b0:a9:d3:0a:ae:fd:9b:7e:88:ed:38:00:56:5d:1e:  
7f:06:33:13:4d:65:19:29:2d:49:bd:55:ec:30:a1:67:19:7f:  
ec:0f:74:29:82:2b:95

## X509v3 extensions:

X509v3 keyUsage:

digitalSignature

X509v3 sbgp-ipAddrBlock:

IPv4:

192.0.2.0/24

198.51.100.0/28

203.0.113.0/24

IPv6:

2001:db8:1234::/48

3fff:600:: - 3fff:fff:ffff:ffff:ffff:ffff:ffff:ffff

X509v3 sbgp-ipAddrBlockV2:

IPv4 unicast:

192.0.2.0/24

198.51.100.0/28

203.0.113.0/24

IPv6 unicast:

2001:db8:1234::/48

3fff:3:: - 3fff:122:0:2233:3344:5566:ffff:ffff

Signature Algorithm: SHA384WITHECDSA

Signature Value:

30:64:02:30:67:09:c9:92:91:9b:49:c4:8f:d9:31:d0:5c:49:  
7d:38:65:e6:08:4c:91:df:3a:4c:7e:78:1f:41:85:43:b0:23:  
d5:9e:8b:f2:5d:13:3f:b1:a0:94:e9:d4:2c:8f:a6:ed:02:30:  
20:ed:9f:db:5a:30:9b:2c:87:04:dd:a5:f1:44:f1:7b:b3:16:  
b9:8c:29:11:24:fb:a5:cf:ec:6e:f9:7f:26:88:06:9a:e6:c5:  
2e:2b:3c:e2:23:12:8d:d1:0c:2a:a7:30

### 3.9.3. C509 Type 3 Certificate

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

Plain hex (405 bytes):

```
0342123401F61A6775D7001A69570A808A01781873656C667369676E2D627261696E
706F6F6C703338347231026A6D79207375726E616D650A686D79207469746C650D6C
6D7920676976656E4E616D651819676D79206E616D6518195861046709C992919B49
C48FD931D05C497D3865E6084C91DF3A4C7E781F418543B023D59E8BF25D133FB1A0
94E9D42C8FA6ED3B46E9883A35ABD4B0A9D30AAEFD9B7E88ED3800565D1E7F063313
4D6519292D49BD55EC30A167197FEC0F7429822B9586020118208601F6831A01C000
021B00000005C47363FE3B00000005C468638E02F6821B000120010DB81234823B00
0120010C78132D091822860101831A01C000021B00000005C47363FE3B00000005C4
68638E020182470020010DB812348245003FFF00034D003FFF012200002233334455
6658606709C992919B49C48FD931D05C497D3865E6084C91DF3A4C7E781F418543B0
23D59E8BF25D133FB1A094E9D42C8FA6ED20ED9FDB5A309B2C8704DDA5F144F17BB3
16B98C291124FBA5CFEC6EF97F2688069AE6C52E2B3CE223128DD10C2AA730
```

Annotated hex:

- \* See the annotated hex for the C509 type 2 certificate in Section 3.9.4. The only differences are the certificate type, the signature value, and the key identifiers.

### 3.9.4. C509 Type 2 Certificate

Plain hex (405 bytes):

```
0242123401F61A6775D7001A69570A808A01781873656C667369676E2D627261696E
706F6F6C703338347231026A6D79207375726E616D650A686D79207469746C650D6C
6D7920676976656E4E616D651819676D79206E616D6518195861046709C992919B49
C48FD931D05C497D3865E6084C91DF3A4C7E781F418543B023D59E8BF25D133FB1A0
94E9D42C8FA6ED3B46E9883A35ABD4B0A9D30AAEFD9B7E88ED3800565D1E7F063313
4D6519292D49BD55EC30A167197FEC0F7429822B9586020118208601F6831A01C000
021B00000005C47363FE3B00000005C468638E02F6821B000120010DB81234823B00
0120010C78132D091822860101831A01C000021B00000005C47363FE3B00000005C4
68638E020182470020010DB812348245003FFF00034D003FFF012200002233334455
6658606709C992919B49C48FD931D05C497D3865E6084C91DF3A4C7E781F418543B0
23D59E8BF25D133FB1A094E9D42C8FA6ED01853890E65008EADDEEAB4914203C9AE8E
C9DA8908B30BFA61E9A1618C2047C3ECF3BAB63E2008D66C9DE3B4F3AE0193
```

Annotated hex:

```
0: 02 # [0]. certificate type=2
1: 42 # [1]. certificateSerialNumber=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 on
curve brainpoolp384r1
92: 58 61 # [8]. subject public key=EC point=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: IPAddrBlocks
196: 86 # value=array[6]
IPAddrBlock[0]
197: 01 # AFI=1: IPv4
198: F6 # SAFI=<null>
199: 83 # IntIPAddressChoice=array[3]
```

```

200: 1A 01C00002 # [0]=AddressPrefix=29360130
205: 1B 00000005C47363FE # [1]=AddressPrefix=24770733054
214: 3B 00000005C468638E # [2]=AddressPrefix=-24770012047
 # IPAddrBlock[1]
223: 02 # AFI=2: IPv6
224: F6 # SAFI=<null>
225: 82 # IntIPAddressChoice=array[2]
226: 1B 000120010DB81234 # [0]=AddressPrefix=3166638739338
 # 76
235: 82 # [1]=AddressRange=array[2]
236: 3B 000120010C78132D # min=-316663852962606
245: 09 # max=9
 # extension[2]
246: 18 22 # type=34: IPAddrBlocksV2
248: 86 # value=array[6]
 # IPAddrBlock[0]
249: 01 # AFI=1: IPv4
250: 01 # SAFI=1: unicast
251: 83 # IntIPAddressChoice=array[3]
252: 1A 01C00002 # [0]=AddressPrefix=29360130
257: 1B 00000005C47363FE # [1]=AddressPrefix=24770733054
266: 3B 00000005C468638E # [2]=AddressPrefix=-24770012047
 # IPAddrBlock[1]
275: 02 # AFI=2: IPv6
276: 01 # SAFI=1: unicast
277: 82 # IPAddressChoice=array[2]
278: 47 # [0]=AddressPrefix=byte[7]
279: 0020010DB81234
286: 82 # [1]=AddressRange=array[2]
287: 45 # min=byte[5]
288: 003FFF0003
293: 4D # max=byte[13]
294: 003FFF01220000223333445566
307: 58 60 # [10]. signature value=byte[96]
309: 6709C992919B49C48FD931D05C497D3865E6084C91DF3A4C7E781F418543
339: B023D59E8BF25D133FB1A094E9D42C8FA6ED01853890E65008EADDEEAB491
369: 4203C9AE8EC9DA8908B30BFA61E9A1618C2047C3ECF3BAB63E2008D66C9D
399: E3B4F3AE0193

```

### 3.10. Weierstrass EC Public Key On Curve brainpoolP512r1

- \* Self-signed certificate
- \* EC public key on the curve brainpoolP512r1
- \* Signature algorithm: ecdsa-with-shake256
- \* Subject:

- jurisdictionCountryName
- jurisdictionStateOrProvinceName
- jurisdictionLocalityName

\* Extensions:

- Subject Directory Attributes
- Subject Information Access
- Policy Mappings

### 3.10.1. Private Key

```
-----BEGIN PRIVATE KEY-----
MGICAQAwFAYHKoZIzj0CAQYJKyQDAwIIAQENBEcwRQIBAQRATz1SqdaOV5JXG3zt
tb9ctxRELipEw4kH0boqayh3PA02UW4leQ6yGuqx7iyWQKOzZYT5tnXlUqGh7jh/
+13K8g==
-----END PRIVATE KEY-----
```

### 3.10.2. X.509 Certificate

PEM content (809 bytes):

```
-----BEGIN CERTIFICATE-----
MIIDJTCCAomgAwIBAgICEjQwCgYIKwYBBQUHBIewgYkxITAfBgNVBAMMGHNlbGZz
aWduLWJyYWlucG9vbHA1MTJyMTEoMCYGCysGAQQBgjc8AgEBDBdteSBqdXJpc2Rp
Y3Rpb25Mb2Nhbg10eTElMCMGCysGAQQBgjc8AgECDBRteSBqdXJpc2RpY3Rpb25T
dGF0ZTETMBEGCysGAQQBgjc8AgEDDAJTRTAeFw0yNTAxMDIwMDAwMDBaFw0yNjAx
MDIwMDAwMDBaMIGJMSEwHwYDVQQDDbhZwXmc2lnbilicmFpbmBvb2xwNTEycjEx
KDAmBgSrBgEEAYI3PAIBAQwXbXkganVyaXNkaWN0aW9uTG9jYWxpdkxkxJTAjBgSr
BgEEAYI3PAIBAgwUbXkganVyaXNkaWN0aW9uU3RhdGUxEzARBgsrBgEEAYI3PAIB
AwwCU0UwgZswFAYHKoZIzj0CAQYJKyQDAwIIAQENA4GCAARtMnBn0zTOU/opMXqi
B7hcojdiPxmhDF1L8CT8P/62T6tYhNDUSKJxVS4C589E2L8QTaGCzsHeiVyEGLhS
nZuLLEuApzbdxWRx1qUsbOQU5p1XNwSV/Aika2H6W3Ifq8dpMvODba3k9w9vDKy4
0zUafrVO/wd8QCNoxJu3FbU0WKOBMzCBmDALBgNVHQ8EBAMCB4AwGgYDVR0JBMMw
ETAPBgNVBAYxCawCREUMAlNFMDMGA1UdIQQsMCowEAYGZ4EMAQICBgZngQwBAgEw
FgYJKwYBBAGB/VkGBgkrBgEEAYH9WQcwOAYIKwYBBQUHAQsELDAqMCgGCCsGAQUF
BzACHhxodHRwOi8vY2Fpc3N1ZXJzLmV4YWlwbGUuY29tMAoGCCsGAQUFBwYhA4GJ
ADCbhQJBAKjwK7Pvesjw+rp+JZFbF+xJvisYgDW/nZyWlMzp5exXNGrRInHSDwy0
CKQVXpuac9bZv627p4Z+DOUxx6/4Cv4CQBt+5b77HaFS0XasMdcu+WbiwPD/tNsZ
Fx6YPBtAcnGbXbrq1LaRuOGjIKX0nvkiqhhVEaPv25rABP8o5V+13Ls=
-----END CERTIFICATE-----
```

Textual Representation:

## Certificate:

Version: v3 (2)

Serial Number:

12:34

Issuer: CN=selfsign-brainpoolp512r1,jurisdictionLocality=my jurisdictionLocality,jurisdictionState=my jurisdictionState,jurisdictionCountry=SE

## Validity:

Not Before: Thu Jan 02 01:00:00 CET 2025

Not After : Fri Jan 02 01:00:00 CET 2026

Subject: CN=selfsign-brainpoolp512r1,jurisdictionLocality=my jurisdictionLocality,jurisdictionState=my jurisdictionState,jurisdictionCountry=SE

## Subject Public Key Info:

Public Key Algorithm: EC/BRAINPOOLP512R1

Pub:

04:6d:32:70:67:d3:34:ce:53:fa:29:31:7a:a2:07:b8:5c:a2:  
37:62:3f:19:a1:0c:59:4b:f0:24:fc:3f:fe:b6:4f:ab:58:84:  
d0:d4:48:a2:71:55:2e:02:e7:cf:44:d8:bf:10:4d:a1:82:ce:  
c1:de:89:5c:84:18:b8:52:9d:9b:8b:2c:4b:80:a7:36:dd:c5:  
64:71:d6:a5:2c:6c:e4:14:e6:9d:57:35:6b:15:fc:08:a4:6b:  
61:fa:5b:72:1f:ab:c7:69:32:f3:83:6d:ad:e4:f7:0f:6f:0c:  
ac:b8:d3:35:1a:7e:b5:4e:ff:07:7c:40:23:68:c4:9b:b7:15:  
b5:34:58

## X509v3 extensions:

X509v3 keyUsage:

digitalSignature

X509v3 subjectDirectoryAttributes:

at-country

DE

SE

X509v3 policyMappings:

2.23.140.1.2.2 : 2.23.140.1.2.1

1.3.6.1.4.1.32473.6 : 1.3.6.1.4.1.32473.7

X509v3 subjectInfoAccess:

CA Issuers: URI: <http://caissuers.example.com>

Signature Algorithm: SHAKE256WITHECDSA

Signature Value:

30:81:85:02:41:00:a8:f0:2b:b3:ef:79:28:f0:fa:ba:7e:25:  
91:5b:17:ec:49:be:24:98:80:35:bf:9d:9c:96:94:cc:e9:e5:  
ec:57:34:6a:d1:22:71:d2:0f:0c:b4:08:a4:15:5e:9b:9a:73:  
d6:d9:bf:ad:bb:a7:86:7e:0c:e5:31:c7:af:f8:0a:fe:02:40:  
1b:7e:e5:be:fb:1d:a1:52:d1:76:ac:31:d7:2e:f9:66:e2:c0:  
f0:ff:b4:db:19:17:1e:98:3c:1b:40:72:71:9b:5d:ba:ea:d4:  
b6:91:b8:e1:a3:20:a5:f4:9e:f9:22:aa:18:55:11:a3:ef:db:  
9a:c0:04:ff:28:e5:5f:a5:dc:bb

## 3.10.3. C509 Type 3 Certificate

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

Plain hex (431 bytes):

```
0342123404F61A6775D7001A69570A808801781873656C667369676E2D627261696E
706F6F6C70353132723113776D79206A7572697364696374696F6E4C6F63616C6974
7914746D79206A7572697364696374696F6E537461746515625345181A5881046D32
7067D334CE53FA29317AA207B85CA237623F19A10C594BF024FC3FFEB64FAB5884D0
D448A271552E02E7CF44D8BF104DA182CEC1DE895C8418B8529D9B8B2C4B80A736DD
C56471D6A52C6CE414E69D57356B15FC08A46B61FA5B721FABC76932F3836DADE4F7
0F6F0CACB8D3351A7EB54EFF077C402368C49BB715B5345888020118188204826244
45625345181B840201492B0601040181FD5906492B0601040181FD5907181F820278
1C687474703A2F2F6361697373756572732E6578616D706C652E636F6D5880A8F02B
B3EF7928F0FABA7E25915B17EC49BE24988035BF9D9C9694CCE9E5EC57346AD12271
D20F0CB408A4155E9B9A73D6D9BFADBBA7867E0CE531C7AFF80AFE1B7EE5BEFB1DA1
52D176AC31D72EF966E2C0F0FFB4DB19171E983C1B4072719B5DBAEAD4B691B8E1A3
20A5F49EF922AA185511A3EFDB9AC004FF28E55FA5DCBB
```

Annotated hex:

- \* See the annotated hex for the C509 type 2 certificate in Section 3.10.4. The only differences are the certificate type, the signature value, and the key identifiers.

## 3.10.4. C509 Type 2 Certificate

Plain hex (431 bytes):

```
0242123404F61A6775D7001A69570A808801781873656C667369676E2D627261696E
706F6F6C70353132723113776D79206A7572697364696374696F6E4C6F63616C6974
7914746D79206A7572697364696374696F6E537461746515625345181A5881046D32
7067D334CE53FA29317AA207B85CA237623F19A10C594BF024FC3FFEB64FAB5884D0
D448A271552E02E7CF44D8BF104DA182CEC1DE895C8418B8529D9B8B2C4B80A736DD
C56471D6A52C6CE414E69D57356B15FC08A46B61FA5B721FABC76932F3836DADE4F7
0F6F0CACB8D3351A7EB54EFF077C402368C49BB715B5345888020118188204826244
45625345181B840201492B0601040181FD5906492B0601040181FD5907181F820278
1C687474703A2F2F6361697373756572732E6578616D706C652E636F6D5880A0B9ED
538672D0B80E48F3D7C4E902503BAC0BDC88B45DAC784DDCFA551AF188B6E2E51F6E
695D7CFC91396BEB17FD91CF9C82D1FB819FEA09C9C4AC9BDCEF1B9AE37BD98556C3
917E9D2FA7327C4FDE6A6CFC99320B3CA097766A9C1A41227A5227CE4F29079B59D5
33DEAFDE51B599B052C91178BE8FA29F86F0FADBC412F9
```

Annotated hex:

```
0: 02 # [0]. certificate type=2
1: 42 # [1]. certificateSerialNumber=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: jurisdictionLocalityName
45: 77 # value=char[23]
46: 6D79206A75726973646963746966F6E4C # "my jurisdictionL"
62: 6F63616C697479 # "ocality"
attribute[2]
69: 14 # type=20: jurisdictionStateOrProvinceName
70: 74 # value=char[20]
71: 6D79206A75726973646963746966F6E53 # "my jurisdictionS"
87: 74617465 # "tate"
attribute[3]
91: 15 # type=21: jurisdictionCountryName
92: 62 # value=char[2]
93: 5345 # "SE"
95: 18 1A # [7]. subjectPublicKeyAlg=26: EC public key on
curve brainpoolp512r1
97: 58 81 # [8]. subject public key=EC point=byte[129]
99: 046D327067D334CE53FA29317AA207B85CA237623F19A10C594BF024FC3F
129: FEB64FAB5884D0D448A271552E02E7CF44D8BF104DA182CEC1DE895C8418
159: B8529D9B8B2C4B80A736DDC56471D6A52C6CE414E69D57356B15FC08A46B
189: 61FA5B721FABC76932F3836DADE4F70F6F0CACB8D3351A7EB54EFF077C40
219: 2368C49BB715B53458
228: 88 # [9]. extensions=array[8]
extension[0]
229: 02 # type=2: KeyUsage
230: 01 # value=1: [digitalSignature]
extension[1]
231: 18 18 # type=24: SubjectDirectoryAttributes
233: 82 # value=array[2], 1 Attribute
234: 04 # attributeType=4: country
235: 82 # attributeValue=array[2]
236: 62 # attributeValue[0]=char[2]
237: 4445 # "DE"
239: 62 # attributeValue[1]=char[2]
```

```

240: 5345 # "SE"
 # extension[2]
242: 18 1B # type=27: PolicyMappings
244: 84 # value=array[4]
 # policyMapping[0]
245: 02 # issuerDomainPolicy=2:
 # organization-validated
246: 01 # subjectDomainPolicy=1:
 # domain-validated
 # policyMapping[1]
247: 49 # issuerDomainPolicy=byte[9]:
248: 2B0601040181FD5906 # oid: 1.3.6.1.4.1.32473.6
257: 49 # subjectDomainPolicy=byte[9]:
258: 2B0601040181FD5907 # oid: 1.3.6.1.4.1.32473.7
 # extension[3]
267: 18 1F # type=31: SubjectInfoAccess
269: 82 # value=array[2]
 # AccessDescription[0]
270: 02 # accessMethod=2: caIssuers
271: 78 1C # uri=char[28]
273: 687474703A2F2F6361697373756572 # "http://caissuer"
288: 732E6578616D706C652E636F6D # "s.example.com"
301: 58 80 # [10]. signature value=byte[128]
303: A0B9ED538672D0B80E48F3D7C4E902503BAC0BDC88B45DAC784DDCFA551A
333: F188B6E2E51F6E695D7CFC91396BEB17FD91CF9C82D1FB819FEA09C9C4AC
363: 9BDCEF1B9AE37BD98556C3917E9D2FA7327C4FDE6A6CFC99320B3CA09776
393: 6A9C1A41227A5227CE4F29079B59D533DEAFDE51B599B052C91178BE8FA2
423: 9F86F0FADBC412F9

```

### 3.11. Weierstrass EC Public Key On Curve frp256v1

- \* Self-signed certificate
- \* EC public key on the curve frp256v1
- \* Signature algorithm: ecdsa-with-sha1
- \* Subject:
  - emailAddress
  - telephoneNumber
  - businessCategory
- \* Extensions:
  - Policy Constraints containing only requireExplicitPolicy

- Name Constraints containing only permittedSubTrees

### 3.11.1. Private Key

```
-----BEGIN PRIVATE KEY-----
MEMCAQAwFQYHkoZIZj0CAQYKKoF6AYFfZYIAAQnMCUCAQEIIjiRO+dimF7NRmd
P/hEljaAZ/C+2RTvYI3Hf8bZUf4h
-----END PRIVATE KEY-----
```

### 3.11.2. X.509 Certificate

PEM content (584 bytes):

```
-----BEGIN CERTIFICATE-----
MIICRDCCAeugAwIBAgICEjQwCQYHkoZIZj0EATB3MR4wHAYJKoZIhvcNAQkBFg9h
YmNAZXhhbXBsZS5vcmcxGjAYBgNVBAMMEXNlbGZzaWduLWZycDI1NnYxMRwwGgYD
VQQPDBNteSBidXNpbmVzc0NhdGVnb3J5MRswGQYDVQQUDBJteSB0ZWxlcGhvbmVO
dWliZXIwHhcNMjUwMTAyMDAwMDAwWhcNMjUwMTAyMDAwMDAwWjB3MR4wHAYJKoZI
hvcNAQkBFg9hYmNAZXhhbXBsZS5vcmcxGjAYBgNVBAMMEXNlbGZzaWduLWZycDI1
NnYxMRwwGgYDVQQUDBNteSBidXNpbmVzc0NhdGVnb3J5MRswGQYDVQQUDBJteSB0
ZWxlcGhvbmVOdWliZXIwWzAVBgqhkJOPQIBBgoqgXoBgV9lggABA0IABDeNLSih
9lRxJPLbakL2ORW/ovZTeuIM8EF9Z1++ZgPagKTPPx5DYzNDqzvoAVDsB0lkndYn
BbwFW9zaer6yUGKjZjBkMAsGA1UdDwQEAwIHgDBHBgNVHR4EQDA+oDwwHIIacGVy
bWl0dGVkLmRuczEuZXhhbXBsZS5jb20wHIIacGVybWl0dGVkLmRuczIuZXhhbXBs
ZS5jb20wDAYDVR0kBAUwA4ABATAJBgcqhkJOPQQA0gAMEUCIDeNLSih9lRxJPLb
akL2ORW/ovZTeuIM8EF9Z1++ZgPaAiEA05r5YOT77AWy1Iik7Z8Bj0ZgxVC8dqcW
8WcF/AjYW9s=
-----END CERTIFICATE-----
```

Textual Representation:

## Certificate:

Version: v3 (2)

Serial Number:

12:34

Issuer: E=abc@example.org,CN=selfsign-frp256v1,BusinessCategory=my  
businessCategory,TelephoneNumber=my telephoneNumber

## Validity:

Not Before: Thu Jan 02 01:00:00 CET 2025

Not After : Fri Jan 02 01:00:00 CET 2026

Subject: E=abc@example.org,CN=selfsign-frp256v1,BusinessCategory=my  
businessCategory,TelephoneNumber=my telephoneNumber

## Subject Public Key Info:

Public Key Algorithm: EC/FRP256V1

Pub:

04:37:8d:2d:28:a1:f6:54:71:24:f2:db:6a:42:f6:39:15:bf:

a2:f6:53:7a:e2:0c:f0:41:7d:67:5f:be:66:03:da:80:a4:cf:

3f:1e:43:63:33:43:ab:3b:e8:01:50:ec:04:e9:64:9d:d6:27:

05:bc:05:5b:dc:da:79:1e:b2:50:62

## X509v3 extensions:

X509v3 keyUsage:

digitalSignature

X509v3 nameConstraints:

Permitted

DNS: permitted.dns1.example.com

DNS: permitted.dns2.example.com

X509v3 policyConstraints:

Require Explicit Policy:1, Inhibit Explicit Policy:null

Signature Algorithm: SHA1WITHECDSA

Signature Value:

30:45:02:20:37:8d:2d:28:a1:f6:54:71:24:f2:db:6a:42:f6:

39:15:bf:a2:f6:53:7a:e2:0c:f0:41:7d:67:5f:be:66:03:da:

02:21:00:d3:9a:f9:60:e4:fb:ec:05:b2:d4:88:a4:ed:9f:01:

8f:46:60:c5:50:bc:76:a7:16:f1:67:05:fc:08:d8:5b:db

### C509 Type 3 Certificate

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

Plain hex (302 bytes):

```

0342123438FEF61A6775D7001A69570A8088006F616263406578616D706C652E6F72
67017173656C667369676E2D66727032353676310B736D7920627573696E65737343
617465676F7279181A726D792074656C6570686F6E654E756D626572181B58410437
8D2D28A1F6547124F2DB6A42F63915BFA2F6537AE20CF0417D675FBE6603DA80A4CF
3F1E43633343AB3BE80150EC04E9649DD62705BC055BDCDA791EB25062860201181A
828402781A7065726D69747465642E646E73312E6578616D706C652E636F6D02781A
7065726D69747465642E646E73322E6578616D706C652E636F6DF6181C8201F65840
378D2D28A1F6547124F2DB6A42F63915BFA2F6537AE20CF0417D675FBE6603DAD39A
F960E4FBEC05B2D488A4ED9F018F4660C550BC76A716F16705FC08D85BDB

```

Annotated hex:

- \* See the annotated hex for the C509 type 2 certificate in Section 3.11.3. The only differences are the certificate type, the signature value, and the key identifiers.

### 3.11.3. C509 Type 2 Certificate

Plain hex (302 bytes):

```

0242123438FEF61A6775D7001A69570A8088006F616263406578616D706C652E6F72
67017173656C667369676E2D66727032353676310B736D7920627573696E65737343
617465676F7279181A726D792074656C6570686F6E654E756D626572181B58410437
8D2D28A1F6547124F2DB6A42F63915BFA2F6537AE20CF0417D675FBE6603DA80A4CF
3F1E43633343AB3BE80150EC04E9649DD62705BC055BDCDA791EB25062860201181A
828402781A7065726D69747465642E646E73312E6578616D706C652E636F6D02781A
7065726D69747465642E646E73322E6578616D706C652E636F6DF6181C8201F65840
378D2D28A1F6547124F2DB6A42F63915BFA2F6537AE20CF0417D675FBE6603DA6F2D
4CE3787CBACE549599BC5F3BAACCA2B7E67352E4A6BA1F4496CEAD53D8E6

```

Annotated hex:

```

0: 02 # [0]. certificate type=2
1: 42 # [1]. certificateSerialNumber=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 on
 # curve frp256v1
98: 58 41 # [8]. subject public key=EC point=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: 78 1A # GeneralNameValue=char[26]
175: 7065726D69747465642E646E73312E # "permitted.dns1."
190: 6578616D706C652E636F6D # "example.com"
 # GeneralName[1]
201: 02 # GeneralNameType=2: dNSName
202: 78 1A # GeneralNameValue=char[26]
204: 7065726D69747465642E646E73322E # "permitted.dns2."
219: 6578616D706C652E636F6D # "example.com"
230: F6 # excludedSubtrees=<null>
 # extension[2]
231: 18 1C # type=28: PolicyConstraints
233: 82 # value=array[2]
234: 01 # requireExplicitPolicy=1
235: F6 # inhibitPolicyMapping=<null>
236: 58 40 # [10]. signature value=byte[64]
238: 378D2D28A1F6547124F2DB6A42F63915BFA2F6537AE20CF0417D675FBE66
268: 03DA6F2D4CE3787CBACE549599BC5F3BAACCA2B7E67352E4A6BA1F4496CE
298: AD53D8E6

```

## 3.12. Montgomery EC Public Key On Curve X25519

- \* X25519 public key
- \* Extensions
  - authorityKeyIdentifier containing only the keyIdentifier component
  - authorityInfoAccess
  - issuerAltName

## 3.12.1. Private Key

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

## 3.12.2. X.509 Certificate

- \* Issued by the CA in Section 2.2.

PEM content (643 bytes):

```
-----BEGIN CERTIFICATE-----
MIICfzCCAmygAwIBAgICEjQwCgYIKwYBBQUHBIQWEjEQMA4GA1UEAwHdGVzdCBj
YTAeFw0yNTAxMDIwMDAwMDBaFw0yNjAxMDIwMDAwMDBaMBQxEjAQBgNVBAMMCWVl
LXgyNTUxOTAqMAUGAytlbGhAIr/UW+scSRBUOcPknf0rff7KfQaekqIKL1HZyL8
G38Io4IB3TCCAdkwCwYDVR0PBAQDAgMoMB8GA1UdIwQYMBaAFH/NuC0ElS4aNrkK
83o88WbRXvkhMIIBkwYIKwYBBQUHAQEegGFMIIBgTAjBggrBgEFBQcwAYYXaHR0
cDovL29jc3AuZXhhbXBsZS5jb20wKAYIKwYBBQUHMAKGHh0dHA6Ly9jYWlzc3Vl
cnMuZXhhbXBsZS5jb20wKwYIKwYBBQUHMAWGH2h0dHA6Ly9jYXJlcG9zaXRvcnku
ZXhhbXBsZS5jb20wKwYIKwYBBQUHMAOGH2h0dHA6Ly90aW1lc3RhbnBpbnRlc3Vl
bXBsZS5jb20wKwYIKwYBBQUHMAWGH2h0dHA6Ly9jYXJlcG9zaXRvcnkuZXhhbXBs
ZS5jb20wKwYIKwYBBQUHMAqGH2h0dHA6Ly9ycGtpbmWFuaWZlc3QuZXhhbXBsZS5j
b20wKwYIKwYBBQUHMAuGH2h0dHA6Ly9zaWduZWVudWV4YXJlc3QuZXhhbXBsZS5j
b20wKwYIKwYBBQUHMA2GHWh0dHA6Ly9ycGtpbm90aWZ5LmV4YWlwbGUuY29tMCQGCSSG
AQQBgflZA4YXaHR0cDovLzEyMzQuZXhhbXBsZS5jb20wEgYDVR0SBAswCYIHYWJj
LmNvbTAKBggrBgEFBQcGJAMBAA==
-----END CERTIFICATE-----
```

Textual Representation:

## Certificate:

Version: v3 (2)

Serial Number:

12:34

Issuer: CN=test ca

Validity:

Not Before: Thu Jan 02 01:00:00 CET 2025

Not After : Fri Jan 02 01:00:00 CET 2026

Subject: CN=ee-x25519

Subject Public Key Info:

Public Key Algorithm: X25519

Pub:

8a:ff:51:6f:ac:71:24:41:50:e7:0f:92:77:f4:ad:f7:fb:29:

f4:1a:7a:4a:88:28:bd:47:67:22:fc:1b:7f:08

X509v3 extensions:

X509v3 keyUsage:

keyEncipherment, keyEncipherment

X509v3 authorityKeyIdentifier:

7f:cd:b8:2d:04:95:2e:1a:36:b9:0a:f3:7a:3c:f1:66:d1:5e:f9:21

X509v3 authorityInfoAccess:

OCSP: URI: http://ocsp.example.com

CA Issuers: URI: http://caissuers.example.com

ad-caRepository: URI: http://carepository.example.com

ad-timeStamping: URI: http://timestamping.example.com

ad-caRepository: URI: http://carepository.example.com

RPKI Manifest: URI: http://rpkimanifest.example.com

Signed Object: URI: http://signedobject.example.com

RPKI Notify: URI: http://rpkinotify.example.com

1.3.6.1.4.1.32473.3: URI: http://1234.example.com

X509v3 issuerAlternativeName:

30:09:82:07:61:62:63:2e:63:6f:6d

Signature Algorithm: unsigned

Signature Value: &lt;empty&gt;

## 3.12.3. C509 Type 3 Certificate

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

Plain hex (398 bytes):

```

034212340567746573742063611A6775D7001A69570A806965652D78323535313908
58208AFF516FAC71244150E70F9277F4ADF7FB29F41A7A4A8828BD476722FC1B7F08
88021407547FCDB82D04952E1A36B90AF37A3CF166D15EF92109920177687474703A
2F2F6F6373702E6578616D706C652E636F6D02781C687474703A2F2F636169737375
6572732E6578616D706C652E636F6D05781F687474703A2F2F63617265706F736974
6F72792E6578616D706C652E636F6D03781F687474703A2F2F74696D657374616D70
696E672E6578616D706C652E636F6D05781F687474703A2F2F63617265706F736974
6F72792E6578616D706C652E636F6D0A781F687474703A2F2F72706B696D616E6966
6573742E6578616D706C652E636F6D0B781F687474703A2F2F7369676E65646F626A
6563742E6578616D706C652E636F6D0D781F687474703A2F2F72706B696E6F746966
792E6578616D706C652E636F6D492B0601040181FD590377687474703A2F2F313233
342E6578616D706C652E636F6D1819676162632E636F6D40

```

Annotated hex:

- \* See the annotated hex for the C509 type 2 certificate in Section 3.12.4. The only differences are the certificate type, the signature value, and the key identifiers.

### 3.12.4. C509 Type 2 Certificate

- \* Issued by the CA in Section 2.4.

Plain hex (398 bytes):

```

024212340567746573742063611A6775D7001A69570A806965652D78323535313908
58208AFF516FAC71244150E70F9277F4ADF7FB29F41A7A4A8828BD476722FC1B7F08
88021407540369D71F96FE1258A746AC2B208E756E6D1D3ED909920177687474703A
2F2F6F6373702E6578616D706C652E636F6D02781C687474703A2F2F636169737375
6572732E6578616D706C652E636F6D05781F687474703A2F2F63617265706F736974
6F72792E6578616D706C652E636F6D03781F687474703A2F2F74696D657374616D70
696E672E6578616D706C652E636F6D05781F687474703A2F2F63617265706F736974
6F72792E6578616D706C652E636F6D0A781F687474703A2F2F72706B696D616E6966
6573742E6578616D706C652E636F6D0B781F687474703A2F2F7369676E65646F626A
6563742E6578616D706C652E636F6D0D781F687474703A2F2F72706B696E6F746966
792E6578616D706C652E636F6D492B0601040181FD590377687474703A2F2F313233
342E6578616D706C652E636F6D1819676162632E636F6D40

```

Annotated hex:

```

0: 02 # [0]. certificate type=2
1: 42 # [1]. certificateSerialNumber=byte[2]
2: 1234
4: 05 # [2]. signature alg=5: unsigned
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: X25519
34: 58 20 # [8]. subject public key=EC point=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=keyIdentifier=byte[20]
73: 0369D71F96FE1258A746AC2B208E756E6D1D3ED9
 # 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: 687474703A2F2F6F6373702E657861 # "http://ocsp.exa"
112: 6D706C652E636F6D # "mple.com"
 # AccessDescription[1]
120: 02 # accessMethod=2: caIssuers
121: 78 1C # uri=char[28]
123: 687474703A2F2F6F6361697373756572 # "http://caissuer"
138: 732E6578616D706C652E636F6D # "s.example.com"
 # AccessDescription[2]
151: 05 # accessMethod=5: caRepository
152: 78 1F # uri=char[31]
154: 687474703A2F2F6F63617265706F7369 # "http://careposi"
169: 746F72792E6578616D706C652E636F # "tory.example.co"
184: 6D # "m"
 # AccessDescription[3]
185: 03 # accessMethod=3: timeStamping
186: 78 1F # uri=char[31]
188: 687474703A2F2F74696D657374616D # "http://timestam"
203: 70696E672E6578616D706C652E636F # "ping.example.co"
218: 6D # "m"
 # AccessDescription[4]
219: 05 # accessMethod=5: caRepository
220: 78 1F # uri=char[31]
222: 687474703A2F2F6F63617265706F7369 # "http://careposi"
237: 746F72792E6578616D706C652E636F # "tory.example.co"
252: 6D # "m"
 # AccessDescription[5]
253: 0A # accessMethod=10: rpkiManifest
```

```

254: 78 1F # uri=char[31]
256: 687474703A2F2F72706B696D616E69 # "http://rpkimani"
271: 666573742E6578616D706C652E636F # "fest.example.co"
286: 6D # "m"
 # AccessDescription[6]
287: 0B # accessMethod=11: signedObject
288: 78 1F # uri=char[31]
290: 687474703A2F2F7369676E65646F62 # "http://signedob"
305: 6A6563742E6578616D706C652E636F # "ject.example.co"
320: 6D # "m"
 # AccessDescription[7]
321: 0D # accessMethod=13: rpkiNotify
322: 78 1D # uri=char[29]
324: 687474703A2F2F72706B696E6F7469 # "http://rpkinoti"
339: 66792E6578616D706C652E636F6D # "fy.example.com"
 # AccessDescription[8]
353: 49 # accessMethod=byte[9]:
354: 2B0601040181FD5903 # oid: 1.3.6.1.4.1.32473.3
363: 77 # uri=char[23]
364: 687474703A2F2F313233342E657861 # "http://1234.exa"
379: 6D706C652E636F6D # "mple.com"
 # extension[3]
387: 18 19 # type=25: IssuerAlternativeName
389: 67 # DNS, value=char[7]
390: 6162632E636F6D # "abc.com"
397: 40 # [10]. signature value=byte[0]

```

### 3.13. Montgomery EC Public Key On Curve X448

- \* X448 public key
- \* Extensions:
  - authorityKeyIdentifier containing all fields
  - crlDistributionPoints
  - freshestCRL

#### 3.13.1. Private Key

```

-----BEGIN PRIVATE KEY-----
MEYCAQAwBQYDK2VvBDoEOPJNe3l0Mqeq8Fwp4DL6opcnehT4qMe0d+/4nSIVodQc
iOJE752KYXs1GZ0/+ETWNoBn8L7ZF09g
-----END PRIVATE KEY-----

```

## 3.13.2. X.509 Certificate

\* Issued by the CA in Section 2.2.

PEM content (518 bytes):

```
-----BEGIN CERTIFICATE-----
MIICAjCCAE+gAwIBAgICEjQwCgYIKwYBBQUHBIQWEjEQMA4GA1UEAwwHdGVzdCBj
YTAeFw0yNTAxMDAwMDBaFw0yNjAxMDIwMDAwMDBaMBIxEDAOBgNVBAMMB2Vl
LXg0NDgwQjAFBgMrZW8DOQAcN++r6pKEezbyZIkK79vJZAocXGGjERwJC+TQpC15
pmZ+K2QnV2D/b9T/A/xZZrUOPZqqy0j006OCAUowggFGMAsgAlUdDwQEAWIDKdAn
BgNVHR8EIDAeMBygGqAYhhZodHRwOi8vY3JsLmV4YWlwbGUuY29tMDoGA1UdIwQz
MDGAFH/NuC0Els4aNrkK83o88WbRXvkhoRakFDASMRawDgYDVQQDDAd0ZXN0IGNh
ggEBMIHRBgNVHS4EgckwgcYwVqAjoCGGH2h0dHA6Ly9mcmVzaGVzdGNYbDEuZXhh
bXBsZS5jb22BAGbAoiukKTAnMQswCQYDVQQGDAJERTEYMBYGA1UEAwwPTXkgQ1JM
IGlzc3VlciAxMGygRqBEhiBodHRwOi8vZnJlc2hlc3RjcmywyMS5leGFtcGxlLmNv
bYYgaHR0cDovL2ZyZXNoZXN0Y3JsMjIuZXhhbXBsZS5jb22BAGECoh6kHDAaMRgw
FgYDVQQDDA9NeSBDbukwgaXNzdWVyIDIwCgYIKwYBBQUHBIQDAQA=
-----END CERTIFICATE-----
```

Textual Representation:

## Certificate:

Version: v3 (2)

Serial Number:

12:34

Issuer: CN=test ca

Validity:

Not Before: Thu Jan 02 01:00:00 CET 2025

Not After : Fri Jan 02 01:00:00 CET 2026

Subject: CN=ee-x448

Subject Public Key Info:

Public Key Algorithm: X448

Pub:

1c:37:ef:ab:ea:92:84:7b:36:f2:64:89:0a:ef:db:c9:64:03:

9c:5c:61:a3:11:1c:09:0b:e4:d0:a4:29:79:a6:66:7e:2b:64:

27:57:60:ff:6f:d4:ff:03:fc:59:66:b5:0e:3d:9a:aa:cb:48:

f4:3b

X509v3 extensions:

X509v3 keyUsage:

keyEncipherment, keyEncipherment

X509v3 cRLDistributionPoints:

Full Name:

URI: http://crl.example.com

X509v3 authorityKeyIdentifier:

7f:cd:b8:2d:04:95:2e:1a:36:b9:0a:f3:7a:3c:f1:66:d1:5e:f9:21

Issuer: Directory Name: CN=test ca

Serial Number:

01

X509v3 freshestCRL:

CRL Issuer:

Directory Name: C=DE,CN=My CRL issuer 1

Reasons: [unused, keyCompromise]

Full Name:

URI: http://freshestcrl1.example.com

CRL Issuer:

Directory Name: CN=My CRL issuer 2

Reasons: [certificateHold]

Full Name:

URI: http://freshestcrl21.example.com

URI: http://freshestcrl22.example.com

Signature Algorithm: unsigned

Signature Value: &lt;empty&gt;

## 3.13.3. C509 Type 3 Certificate

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

Plain hex (301 bytes):

```

034212340567746573742063611A6775D7001A69570A806765652D78343438095838
1C37EFABEA92847B36F264890AEFDBC964039C5C61A3111C090BE4D0A42979A6667E
2B64275760FF6FD4FF03FC5966B50E3D9AAACB48F43B8802140576687474703A2F2F
63726C2E6578616D706C652E636F6D0783547FCDB82D04952E1A36B90AF37A3CF166
D15EF921820467746573742063614101181D8283781F687474703A2F2F6672657368
65737463726C312E6578616D706C652E636F6D038404624445016F4D792043524C20
697373756572203183827820687474703A2F2F667265736865737463726C32312E65
78616D706C652E636F6D7820687474703A2F2F667265736865737463726C32322E65
78616D706C652E636F6D18406F4D792043524C20697373756572203240

```

Annotated hex:

- \* See the annotated hex for the C509 type 2 certificate in Section 3.13.4. The only differences are the certificate type, the signature value, and the key identifiers.

### 3.13.4. C509 Type 2 Certificate

- \* Issued by the CA in Section 2.4.

Plain hex (301 bytes):

```

024212340567746573742063611A6775D7001A69570A806765652D78343438095838
1C37EFABEA92847B36F264890AEFDBC964039C5C61A3111C090BE4D0A42979A6667E
2B64275760FF6FD4FF03FC5966B50E3D9AAACB48F43B8802140576687474703A2F2F
63726C2E6578616D706C652E636F6D0783540369D71F96FE1258A746AC2B208E756E
6D1D3ED9820467746573742063614101181D8283781F687474703A2F2F6672657368
65737463726C312E6578616D706C652E636F6D038404624445016F4D792043524C20
697373756572203183827820687474703A2F2F667265736865737463726C32312E65
78616D706C652E636F6D7820687474703A2F2F667265736865737463726C32322E65
78616D706C652E636F6D18406F4D792043524C20697373756572203240

```

Annotated hex:

```

0: 02 # [0]. certificate type=2
1: 42 # [1]. certificateSerialNumber=byte[2]
2: 1234
4: 05 # [2]. signature alg=5: unsigned
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=EC point=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: 76 # value=fullName=char[22]
95: 687474703A2F2F63726C2E6578616D70 # "http://crl.examp"
111: 6C652E636F6D # "le.com"
 # extension[2]
117: 07 # type=7: AuthorityKeyIdentifier
118: 83 # value=array[3]
119: 54 # keyIdentifier=byte[20]
120: 0369D71F96FE1258A746AC2B208E756E6D1D3ED9
140: 82 # authorityCertIssuer=array[2]
 # GeneralName[0]
141: 04 # GeneralNameType=4: directoryName
142: 67 # GeneralNameValue=char[7]
143: 74657374206361 # "test ca"
150: 41 # authorityCertSerialNumber=byte[1]
151: 01
 # extension[3]
152: 18 1D # type=29: FreshestCRL
154: 82 # value=array[2]
155: 83 # DistributionPoint[0]=array[3]
156: 78 1F # [0]=fullName=char[31]
158: 687474703A2F2F6672657368657374 # "http://freshest"
173: 63726C312E6578616D706C652E636F # "crl1.example.co"
188: 6D # "m"
189: 03 # [1]=reasons3: [unused, keyCompromise]
190: 84 # [2]=CRLIssuer=array[4], 2 attributes
 # attribute[0]
191: 04 # type=4: country
192: 62 # value=char[2]
193: 4445 # "DE"
 # attribute[1]
195: 01 # type=1: commonName
196: 6F # value=char[15]
197: 4D792043524C2069737375657220 # "My CRL issuer "
211: 31 # "1"
212: 83 # DistributionPoint[1]=array[3]
213: 82 # [0]=fullName=array[2]
214: 78 20 # char[32]
216: 687474703A2F2F6672657368657374 # "http://freshest"
231: 63726C32312E6578616D706C652E63 # "crl21.example.c"
246: 6F6D # "om"
248: 78 20 # char[32]

```

```

250: 687474703A2F2F6672657368657374 # "http://freshest"
265: 63726C32322E6578616D706C652E63 # "crl22.example.c"
280: 6F6D # "om"
282: 18 40 # [1]=reasons64: [certificateHold]
284: 6F # [2]=cRLIssuer=char[15]
285: 4D792043524C206973737565722032 # "My CRL issuer 2"
300: 40 # [10]. signature value=byte[0]

```

### 3.14. Edwards EC Public Key On Curve ED25519

- \* Self-signed certificate
- \* Edwards public key Ed25519
- \* Signature algorithm: ed25519
- \* Subject:
  - domainComponent
  - dnQualifier
  - dmdName
  - unstructuredName
  - unstructuredAddress
  - generationQualifier
- \* Extensions:
  - Policy Constraints containing both requireExplicitPolicy and inhibitPolicyMapping
  - Name Constraints containing both permittedSubTrees and excludedSubTrees

#### 3.14.1. Private Key

```

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

```

#### 3.14.2. X.509 Certificate

PEM content (784 bytes):

Textual Representation:

## Certificate:

Version: v3 (2)

Serial Number:

12:34

Issuer: CN=selfsign-ed25519, GENERATION=my generationQualifier, DN=my  
dnQualifier, DC=my domainComponent, 2.5.4.54=my dmdName, unstr  
ucturedName=my unstructuredName, unstructuredAddress=my uns  
tructuredAddress

## Validity:

Not Before: Thu Jan 02 01:00:00 CET 2025

Not After : Fri Jan 02 01:00:00 CET 2026

Subject: CN=selfsign-ed25519, GENERATION=my generationQualifier, DN=m  
y dnQualifier, DC=my domainComponent, 2.5.4.54=my dmdName, un  
structuredName=my unstructuredName, unstructuredAddress=my  
unstructuredAddress

## Subject Public Key Info:

Public Key Algorithm: ED25519

Pub:

46:27:0a:ec:0f:32:83:7e:12:87:79:d3:0b:24:9c:53:1d:6d:

42:c1:ac:29:e4:02:32:8e:dc:79:fa:c2:be:95

## X509v3 extensions:

X509v3 keyUsage:

digitalSignature

X509v3 nameConstraints:

Permitted

DNS: permitted.dns1.example.com

DNS: permitted.dns2.example.com

Excluded

DNS: excluded.dns1.example.com

DNS: excluded.dns2.example.com

X509v3 policyConstraints:

Require Explicit Policy:1, Inhibit Explicit Policy:2

Signature Algorithm: ED25519

Signature Value:

3a:fc:39:99:7c:0d:c7:99:e5:9c:97:29:99:41:0a:b9:78:68:

48:3c:d2:22:bf:92:f0:6b:6a:2c:45:9f:2c:0b:13:4f:7c:90:

1e:24:86:2d:fc:5e:ae:cc:8b:a8:8d:b5:d2:80:ea:8a:4a:97:

3b:fa:4d:d0:3d:0e:2b:d3:68:09

## 3.14.3. C509 Type 3 Certificate

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

Plain hex (383 bytes):

```

034212340CF61A6775D7001A69570A808E017073656C667369676E2D656432353531
390F766D792067656E65726174696F6E5175616C6966696572106E6D7920646E5175
616C696669657216726D7920646F6D61696E436F6D706F6E656E74181B6A6D792064
6D644E616D65181D736D7920756E737472756374757265644E616D65181E766D7920
756E73747275637475726564416464726573730C582046270AEC0F32837E128779D3
0B249C531D6D42C1AC29E402328EDC79FAC2BE95860201181A828402781A7065726D
69747465642E646E73312E6578616D706C652E636F6D02781A7065726D6974746564
2E646E73322E6578616D706C652E636F6D840278196578636C756465642E646E7331
2E6578616D706C652E636F6D0278196578636C756465642E646E73322E6578616D70
6C652E636F6D181C82010258403AFC39997C0DC799E59C972999410AB97868483CD2
22BF92F06B6A2C459F2C0B134F7C901E24862DFC5EAECC8BA88DB5D280EA8A4A973B
FA4DD03D0E2BD36809

```

Annotated hex:

- \* See the annotated hex for the C509 type 2 certificate in Section 3.14.4. The only differences are the certificate type, the signature value, and the key identifiers.

#### 3.14.4. C509 Type 2 Certificate

Plain hex (383 bytes):

```

024212340CF61A6775D7001A69570A808E017073656C667369676E2D656432353531
390F766D792067656E65726174696F6E5175616C6966696572106E6D7920646E5175
616C696669657216726D7920646F6D61696E436F6D706F6E656E74181B6A6D792064
6D644E616D65181D736D7920756E737472756374757265644E616D65181E766D7920
756E73747275637475726564416464726573730C582046270AEC0F32837E128779D3
0B249C531D6D42C1AC29E402328EDC79FAC2BE95860201181A828402781A7065726D
69747465642E646E73312E6578616D706C652E636F6D02781A7065726D6974746564
2E646E73322E6578616D706C652E636F6D840278196578636C756465642E646E7331
2E6578616D706C652E636F6D0278196578636C756465642E646E73322E6578616D70
6C652E636F6D181C8201025840213CF14F253BCECA58A1CDF0AAD3565E01D6612461
F86DBACC6E0140995AC3EEF507AF1341D604243751562CCB363B0C72C989E9D2F260
C594228342AFAC7B00

```

Annotated hex:

```

0: 02 # [0]. certificate type=2
1: 42 # [1]. certificateSerialNumber=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: 6D7920756E7374727563747572656441 # "my unstructuredA"
149: 646472657373 # "ddress"
155: 0C # [7]. subjectPublicKeyAlg=12: Ed25519
156: 58 20 # [8]. subject public key=EC point=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: 78 1A # GeneralNameValue=char[26]
200: 7065726D69747465642E646E73312E # "permitted.dns1."
215: 6578616D706C652E636F6D # "example.com"
```

```

GeneralName[1]
226: 02 # GeneralNameType=2: dNSName
227: 78 1A # GeneralNameValue=char[26]
229: 7065726D69747465642E646E73322E # "permitted.dns2."
244: 6578616D706C652E636F6D # "example.com"
255: 84 # excludedSubtrees=array[4]
GeneralName[0]
256: 02 # GeneralNameType=2: dNSName
257: 78 19 # GeneralNameValue=char[25]
259: 6578636C756465642E646E73312E65 # "excluded.dns1.e"
274: 78616D706C652E636F6D # "xample.com"
GeneralName[1]
284: 02 # GeneralNameType=2: dNSName
285: 78 19 # GeneralNameValue=char[25]
287: 6578636C756465642E646E73322E65 # "excluded.dns2.e"
302: 78616D706C652E636F6D # "xample.com"
extension[2]
312: 18 1C # type=28: PolicyConstraints
314: 82 # value=array[2]
315: 01 # requireExplicitPolicy=1
316: 02 # inhibitPolicyMapping=2
317: 58 40 # [10]. signature value=byte[64]
319: 213CF14F253BCECA58A1CDF0AAD3565E01D6612461F86DBACC6E0140995A
349: C3EEF507AF1341D604243751562CCB363B0C72C989E9D2F260C594228342
379: AFAC7B00

```

### 3.15. Edwards EC Public Key On Curve ED448

- \* Self-signed certificate
- \* Edwards public key Ed448
- \* Signature algorithm: ed448
- \* Subject:
  - initials
  - pseudonym
  - userId
- \* Extensions:
  - OCSP No Check
  - TLS Features

### 3.15.1. Private Key

```
-----BEGIN PRIVATE KEY-----
MEcCAQAwBQYDK2VxBDsEOfJNE3l0Mqeq8Fwp4DL6opcnehT4qMe0d+/4nSIVodQc
iOJE752KYXs1GZ0/+ETWNoBn8L7ZF09gjQ==
-----END PRIVATE KEY-----
```

### 3.15.2. X.509 Certificate

PEM content (503 bytes):

```
-----BEGIN CERTIFICATE-----
MIIB8zCCAXOgAwIBAgICEjQwBQYDK2VxMGExFzAVBgNVBAMMDnNlbGZzaWduLWVkbG90eS0yMDE5MTA1MDUwMTk1NDQ0MRQwEgYDVQQrDAtteSBpbml0aWFnsczEVMBMGAlUEQQwMbXkgcHNldWRvbnltMRkwFwYKczImiZPyLGQBAQwJbXkgdXNlcmlkMKB4XDTI1MDEwMjAwMDAwMFoXDTI1MDEwMjAwMDAwMFowYTEEXBUGAlUEAwWoc2VsZnNpZ24tZWQ0NDgxFDASBgNVBCSMC215IGluaXRpYWxzMRUwEwYDVQRBDAXteSBwc2VlZG9ueW0xGTAXBgoJKiaJk/IsZAEBDAIteSB1c2VyawQwQzAFBgMrZXEDOGCMNeSR21hwLXuZFwnW+Gsmgeol0h+rG7HgECpBBFPyx3PI59sTYRRR/fiJ5Ookan5yl0eIKc5jICjNjA0MASGA1UdDwQEAWIHgDAPBgkrBgEFBQcwAUQUEAgUAMBQGccSGAQUFBWeyBAGwBgIBLAIBEDAFBgMrZXEDcwAiYFAExQwfWAUK3hZXBgg0xcng4EH5i+naHJ0qVXSz/uZN4Q4J39t41FzanofvtGpcNsrrJo6R9lYA7hrTcjMhmMdKYWFUQC4/tKR9evXD+ksKC5cQDK0NeylvE9mClhbRla9lHlk7VwgFTHWIqaQMQA=
-----END CERTIFICATE-----
```

Textual Representation:

## Certificate:

Version: v3 (2)

Serial Number:

12:34

Issuer: CN=selfsign-ed448,INITIALS=my initials,Pseudonym=my pseudonym,UID=my userid

## Validity:

Not Before: Thu Jan 02 01:00:00 CET 2025

Not After : Fri Jan 02 01:00:00 CET 2026

Subject: CN=selfsign-ed448,INITIALS=my initials,Pseudonym=my pseudonym,UID=my userid

## Subject Public Key Info:

Public Key Algorithm: ED448

Pub:

8c:35:e4:91:db:58:70:2d:7b:99:16:7c:19:f8:6b:26:81:ea:

25:d2:1f:83:ac:6e:c7:80:40:a9:04:11:4f:cb:1d:cf:23:9f:

6c:4d:84:51:47:f7:e2:27:93:a8:91:a9:f9:ca:5d:1e:20:a7:

39:8c:80

## X509v3 extensions:

X509v3 keyUsage:

digitalSignature

X509v3 pkix-ocsp-nocheck:

NULL

X509v3 pe-tlsfeature:

44

16

Signature Algorithm: ED448

## Signature Value:

08:c8:50:04:c5:0c:1f:58:05:0a:de:16:57:06:0a:b4:c5:c9:

e0:e0:41:f9:8b:e9:c0:1c:9d:2a:55:74:b3:fe:e6:4d:e1:0e:

09:df:db:78:d4:56:5a:9e:87:ef:b4:6a:5c:36:ca:c9:a3:a4:

7d:95:80:3b:86:b4:dc:8c:c8:4c:74:a6:16:64:55:10:0b:8f:

ed:29:16:bd:7a:f5:c3:fa:4b:0a:0b:97:10:0c:ad:0d:7b:29:

55:7b:d9:82:d6:10:6b:94:0f:75:1e:52:bb:57:08:05:4c:7c:

08:a8:a6:90:31:00

## 3.15.3. C509 Type 3 Certificate

- \* C509 type 3 certificate converted from the X.509 certificate in Section 3.15.2.

Plain hex (260 bytes):

```
034212340DF61A6775D7001A69570A8088016E73656C667369676E2D65643434380E
6B6D7920696E697469616C73116C6D792070736575646F6E796D181C696D79207573
657269640D58398C35E491DB58702D7B99167C19F86B2681EA25D21F83AC6EC78040
A904114FCB1DCF239F6C4D845147F7E22793A891A9F9CA5D1E20A7398C8086020118
24F6182682182C10587208C85004C50C1F58050ADE1657060AB4C5C9E0E041F98BE9
C01C9D2A5574B3FEE64DE10E09DFDB78D4565A9E87EFB46A5C36CAC9A3A47D95803B
86B4DC8CC84C74A6166455100B8FED2916BD7AF5C3FA4B0A0B97100CAD0D7B29557B
D982D6106B940F751E52BB5708054C7C08A8A6903100
```

Annotated hex:

- \* See the annotated hex for the C509 type 2 certificate in Section 3.15.4. The only differences are the certificate type, the signature value, and the key identifiers.

### 3.15.4. C509 Type 2 Certificate

Plain hex (260 bytes):

```
024212340DF61A6775D7001A69570A8088016E73656C667369676E2D65643434380E
6B6D7920696E697469616C73116C6D792070736575646F6E796D181C696D79207573
657269640D58398C35E491DB58702D7B99167C19F86B2681EA25D21F83AC6EC78040
A904114FCB1DCF239F6C4D845147F7E22793A891A9F9CA5D1E20A7398C8086020118
24F6182682182C1058725E12D7D2F577CBDB36BA15DD9EA97B9BB9B49284210308CC
FB2B1C2F9E2FF80398CC5D4F50293AFD24C5BCE3569379D344BCC4D31C6062A400EC
582489B9F8B8CDCF0F4F2C2C38482A6201B78D9B222B8E7CF75431BDBE4FA9061B06
6DA656B5509F36D6005D0C2B602018B79E79C9A20A00
```

Annotated hex:

```
0: 02 # [0]. certificate type=2
1: 42 # [1]. certificateSerialNumber=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: 0D # [7]. subjectPublicKeyAlg=13: Ed448
73: 58 39 # [8]. subject public key=EC point=byte[57]
75: 8C35E491DB58702D7B99167C19F86B2681EA25D21F83AC6EC78040A90411
105: 4FCB1DCF239F6C4D845147F7E22793A891A9F9CA5D1E20A7398C80
132: 86 # [9]. extensions=array[6]
extension[0]
133: 02 # type=2: KeyUsage
134: 01 # value=1: [digitalSignature]
extension[1]
135: 18 24 # type=36: OCSPNoCheck
137: F6 # value=<null>
extension[2]
138: 18 26 # type=38: TLSFeatures
140: 82 # value=array[2]
141: 18 2C # value=44: cookie
143: 10 # value=16: application layer protocol
negotiation
144: 58 72 # [10]. signature value=byte[114]
146: 5E12D7D2F577CBDB36BA15DD9EA97B9BB9B49284210308CCFB2B1C2F9E2F
176: F80398CC5D4F50293AFD24C5BCE3569379D344BCC4D31C6062A400EC5824
206: 89B9F8B8CDCF0F4F2C2C38482A6201B78D9B222B8E7CF75431BDBE4FA906
236: 1B066DA656B5509F36D6005D0C2B602018B79E79C9A20A00
```

#### 4. Certificates With Different Signature Algorithms

##### 4.1. RSASSA-PKCS1-v1\_5 With SHA-1

- \* Self-signed certificate
- \* 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-----
MIIByzCCATSgAwIBAgICEjQwDQYJKoZIhvcNAQEFBQAwITEfMB0GA1UEAwWc2Vs
ZnNpZ24tcnNhLXdpdGgtc2hhMTAeFw0yNTAxMDIwMDAwMDBaFw0yNjAxMDIwMDAw
MDBaMCEwH2AdBgNVBAMMFmNlbGZzaWduLXJzYS13aXRoLXNoYTEwgZ8wDQYJKoZI
hvcNAQEBBQADgY0AMIGJAoGBALgJL28EcmqSHPqy0xOunS8Bx85GX6t9pix6XHP6
zl/7ovHdgKKa3EM5nPyiInm4miZIEOW5JrteDT9yenY+FgE/ifj+rFnQ+9leiwxS
gn5UkPE7hMNjTonG0XMa5fGmD4jtEY0IDhqyyqUy0GwvfSoIdN7k5rblcoP2R42v
QlPbAgMBAAGjEjAQMAGAlUdDWEB/wQEAWIHgDANBgkqhkiG9w0BAQUFAAOBgQBy
vlKYpmd/Cnh0eiiaEvGVVbFQY6Qx95k5BpyVL+Wp2K5oB/WZ5fwP/mf/w8viB7hc
rTO02AaTvV5NJNyt3ubIwV1UBnlMX+OWC43HH6GRH+6cndHiE/2cAKRoGMBA3xKp
4YMRr/kweqpFcIWfFObSWJ4aWdmw/6eg5e3uPIhd/A==
-----END CERTIFICATE-----
```

Textual Representation:

## Certificate:

Version: v3 (2)

Serial Number:

12:34

Issuer: CN=selfsign-rsa-with-sha1

Validity:

Not Before: Thu Jan 02 01:00:00 CET 2025

Not After : Fri Jan 02 01:00:00 CET 2026

Subject: CN=selfsign-rsa-with-sha1

Subject Public Key Info:

Public Key Algorithm: 1.2.840.113549.1.1.1

Pub:

30:81:89:02:81:81:00:b8:09:2f:6f:04:72:6a:92:1c:fa:b2:  
d3:13:ae:9d:2f:01:c7:ce:46:5f:ab:7d:a6:2c:7a:5c:73:fa:  
ce:5f:fb:a2:f1:dd:80:a2:9a:dc:43:39:9c:fc:a2:22:79:b8:  
9a:26:48:10:e5:b9:26:bb:5e:0d:3f:72:7a:76:3e:16:01:3f:  
89:f8:fe:ac:59:d0:fb:dd:5e:8b:0c:52:82:7e:54:90:f1:3b:  
84:c3:63:4e:89:c6:d1:73:1a:e5:f1:a6:0f:88:ed:11:8d:08:  
0e:1a:b2:ca:a5:32:d0:6c:2f:7d:2a:08:74:de:e4:e6:b6:e5:  
72:83:f6:47:8d:af:42:53:db:02:03:01:00:01

X509v3 extensions:

X509v3 keyUsage: critical

digitalSignature

Signature Algorithm: SHA1WITHRSA

Signature Value:

72:be:52:98:a6:67:7f:0a:78:74:7a:28:9a:12:f1:95:55:b1:  
50:63:a4:31:f7:99:39:06:9c:95:2f:e5:a9:d8:ae:68:07:f5:  
99:e5:fc:0f:fe:67:ff:c3:cb:e2:07:b8:5c:ad:33:b4:d8:06:  
93:be:fe:4d:24:dc:ad:de:e6:c8:c1:5d:54:06:7d:4c:5f:e3:  
96:0b:8d:c7:1f:a1:91:1f:ee:9c:9d:d1:e2:13:fd:9c:00:a4:  
68:18:c0:40:df:12:a9:e1:83:11:af:f9:30:7a:aa:45:70:85:  
9f:14:e6:d2:58:9e:1a:59:d9:b0:ff:a7:a0:e5:ed:ee:3c:88:  
5d:fc

## 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 for the C509 type 2 certificate in Section 4.1.4. The only differences are the certificate type, the signature value, and the key identifiers.

#### 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]. certificateSerialNumber=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=modulus=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 3.11.

#### 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 3.5.

## 4.5. ECDSA With SHA512

- \* Signature algorithm: ecdsa-with-sha512

See Section 3.6.

## 4.6. ECDSA With SHAKE128

- \* Signature algorithm: ecdsa-with-shake128

See Section 3.8.

## 4.7. ECDSA With SHAKE256

- \* Signature algorithm: ecdsa-with-shake256

See Section 3.10.

## 4.8. Unsigned

- \* Signature algorithm: unsigned

See Section 2.

## 4.9. SM2 With SM3

- \* Signature algorithm: sm2-with-sm3

See Section 3.7.

## 4.10. Ed25519

- \* Signature algorithm: ed25519

See Section 3.14.

## 4.11. Ed448

- \* Signature algorithm: ed448

See Section 3.15.

## 4.12. ECDH PoP With SHA-256 And HMAC-SHA256

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

See Section 8.3.

## 4.13. ECDH PoP With SHA-384 And HMAC-SHA384

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

See Section 8.4.

## 4.14. ECDH PoP With SHA-512 And HMAC-SHA512

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

See Section 8.5.

## 4.15. RSASSA-PKCS1-v1\_5 With SHA-256

- \* Signature algorithm: sha256WithRSAEncryption

See Section 3.1.

## 4.16. RSASSA-PKCS1-v1\_5 With SHA-384

- \* Signature algorithm: sha384WithRSAEncryption

See Section 3.2.

## 4.17. RSASSA-PKCS1-v1\_5 With SHA-512

- \* Self-signed certificate
- \* Signature algorithm: sha512WithRSAEncryption

## 4.17.1. Private Key

See Section 3.1.1.

## 4.17.2. X.509 Certificate

PEM content (467 bytes):

-----BEGIN CERTIFICATE-----

```
MIIBzzCCATigAwIBAgICEjQwDQYJKoZIhvcNAQENBQAwIzEhMB8GA1UEAwwYc2Vs
ZnNpZ24tcnNhLXdpdGgtc2hhNTEyMB4XDTI1MDEwMjAwMDAwMFoXDTI1MDEwMjAw
MDAwMFowIzEhMB8GA1UEAwwYc2VsZnNpZ24tcnNhLXdpdGgtc2hhNTEyMIGfMA0G
CSqGSIB3DQEBAQUAA4GNADCBiQKBgQC4CS9vBHJqkhz6stMTrp0vAcfORl+rfaYs
elxz+s5f+6Lx3YCimtxDOZz8oiJ5uJomSBDluSa7Xg0/cnp2PhYBP4n4/qxZ0Pvd
XosMUoJ+VJDxO4TDY06JxtFzGuXxpg+I7RGNCA4assqlMtBsL30qCHTe50a25XKD
9keNr0JT2wIDAQABoxIwEDAObgNVHQ8BAf8EBAMCB4AwDQYJKoZIhvcNAQENBQAD
gYEAJAbODIhhp4VHV8H6LZ5YI4CFgBdOg8lrlnTBlpBetrwI7NCEha/22u5epjzv
ZvdYOXLcsvKhqhs2hMGjOVS7R6ffu/9N/nUSa9341ocG/SbeZuXL8Ba12faHGMq2
6yK9i42EI9lvKGUHiXw6WONk8GAXXFHdH6xgTJ/1U2krm+4=
```

-----END CERTIFICATE-----

Textual Representation:

Certificate:

Version: v3 (2)

Serial Number:

12:34

Issuer: CN=selfsign-rsa-with-sha512

Validity:

Not Before: Thu Jan 02 01:00:00 CET 2025

Not After : Fri Jan 02 01:00:00 CET 2026

Subject: CN=selfsign-rsa-with-sha512

Subject Public Key Info:

Public Key Algorithm: 1.2.840.113549.1.1.1

Pub:

```
30:81:89:02:81:81:00:b8:09:2f:6f:04:72:6a:92:1c:fa:b2:
d3:13:ae:9d:2f:01:c7:ce:46:5f:ab:7d:a6:2c:7a:5c:73:fa:
ce:5f:fb:a2:f1:dd:80:a2:9a:dc:43:39:9c:fc:a2:22:79:b8:
9a:26:48:10:e5:b9:26:bb:5e:0d:3f:72:7a:76:3e:16:01:3f:
89:f8:fe:ac:59:d0:fb:dd:5e:8b:0c:52:82:7e:54:90:f1:3b:
84:c3:63:4e:89:c6:d1:73:1a:e5:f1:a6:0f:88:ed:11:8d:08:
0e:1a:b2:ca:a5:32:d0:6c:2f:7d:2a:08:74:de:e4:e6:b6:e5:
72:83:f6:47:8d:af:42:53:db:02:03:01:00:01
```

X509v3 extensions:

X509v3 keyUsage: critical

digitalSignature

Signature Algorithm: SHA512WITHRSA

Signature Value:

```
24:06:ce:0c:88:61:a7:85:47:57:c1:fa:2d:9e:58:23:80:85:
80:17:4e:83:c9:6b:96:74:c1:96:90:5e:b6:bc:08:ec:d0:84:
85:af:f6:da:ee:5e:a6:3c:ef:66:f7:58:39:72:dc:b2:f2:a1:
aa:14:b6:84:c1:a3:39:54:bb:47:a7:df:bb:ff:4d:fe:75:12:
6b:dd:f8:d6:87:06:fd:26:de:66:e5:cb:f0:16:b5:d9:f6:87:
18:ca:b6:eb:22:bd:8b:8d:84:23:dd:6f:28:6b:87:21:7c:3a:
58:e3:64:f0:60:17:5c:51:dd:1f:ac:60:4c:9f:f5:53:69:2b:
9b:ee
```

## 4.17.3. C509 Type 3 Certificate

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

Plain hex (305 bytes):

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

Annotated hex:

- \* See the annotated hex for the C509 type 2 certificate in Section 4.17.4. The only differences are the certificate type, the signature value, and the key identifiers.

## 4.17.4. 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]. certificateSerialNumber=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=modulus=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

```

#### 4.18. RSASSA-PSS With SHA-256

- \* Self-signed certificate
- \* Signature algorithm: rsassa-pss-with-sha256

##### 4.18.1. Private Key

See Section 3.1.1.

##### 4.18.2. X.509 Certificate

PEM content (575 bytes):

-----BEGIN CERTIFICATE-----

MIICozCCAXCgAwIBAgICEjQwQQYJKoZIhvcNAQEKMSgDzANBgglghkgBZQMEAgEF  
AKEcMBoGCSqGSib3DQEBCDANBgglghkgBZQMEAgEFAKIDAgEgMCUxIzAhBgNVBAMM  
GnNlbGZzaWduLXJzYXNzYS1wc3Mtc2hhMjU2MB4XDTI1MDEwMjAwMDAwMFoXDTI2  
MDEwMjAwMDAwMFowJTEjMCEGA1UEAwac2VsZnNpZ24tcnNhcnNhLXBzcy1zaGEy  
NTYwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALgJL28EcmqSHPqy0xOunS8B  
x85GX6t9pix6XHP6zl/7ovHdgKka3EM5nPyiInm4miZIEOW5JrteDT9yenY+FgE/  
ifj+rFnQ+9leiwxSgn5UkPE7hMNjTonG0XMa5fGmD4jtEY0IDhqyyqUy0GwvfSoI  
dN7k5rblcoP2R42vQlPbAgMBAAGjEjAQMA4GA1UdDwEB/wQEAwIHgDBBBgkqhkiG  
9w0BAQowNKAPMA0GCWCGSAFlAwQCAQUAoRwwGgYJKoZIhvcNAQEIIMA0GCWCGSAFl  
AwQCAQUAogMCASADgYEAaxYseZDcSnGCKNIuIk3zWqHnUZIwyOtSrx6iG2RBexZj  
Hr8Gp9Anfzk5p8iw//TcfIkbJl19gfUpdZhxvMQjq6NRqDlHj/gte0npsFtSojF  
7zIGqFbtuwnr3PUKXa8Y/Yu0QBRvw3bZCVNxeixHr1O71t6oJLfEHm6QSXQv+c=

-----END CERTIFICATE-----

Textual Representation:

## Certificate:

Version: v3 (2)

Serial Number:

12:34

Issuer: CN=selfsign-rsassa-pss-sha256

Validity:

Not Before: Thu Jan 02 01:00:00 CET 2025

Not After : Fri Jan 02 01:00:00 CET 2026

Subject: CN=selfsign-rsassa-pss-sha256

Subject Public Key Info:

Public Key Algorithm: 1.2.840.113549.1.1.1

Pub:

30:81:89:02:81:81:00:b8:09:2f:6f:04:72:6a:92:1c:fa:b2:  
d3:13:ae:9d:2f:01:c7:ce:46:5f:ab:7d:a6:2c:7a:5c:73:fa:  
ce:5f:fb:a2:f1:dd:80:a2:9a:dc:43:39:9c:fc:a2:22:79:b8:  
9a:26:48:10:e5:b9:26:bb:5e:0d:3f:72:7a:76:3e:16:01:3f:  
89:f8:fe:ac:59:d0:fb:dd:5e:8b:0c:52:82:7e:54:90:f1:3b:  
84:c3:63:4e:89:c6:d1:73:1a:e5:f1:a6:0f:88:ed:11:8d:08:  
0e:1a:b2:ca:a5:32:d0:6c:2f:7d:2a:08:74:de:e4:e6:b6:e5:  
72:83:f6:47:8d:af:42:53:db:02:03:01:00:01

X509v3 extensions:

X509v3 keyUsage: critical

digitalSignature

Signature Algorithm: SHA256WITHRSAANDMGF1

Signature Value:

6b:16:2c:79:90:dc:4a:71:82:28:d2:2e:22:4d:f3:5a:a1:e7:  
51:92:30:c8:eb:52:af:1e:a2:1b:64:41:7b:16:63:1e:bf:06:  
a7:d0:27:7f:39:39:a7:c8:b0:ff:f4:dc:7c:89:1b:27:5d:7d:  
81:f5:29:75:98:71:bc:c4:23:aa:ae:8d:46:a0:f5:1e:3f:e0:  
b5:ed:27:a6:c1:6d:4a:88:c5:ef:32:06:a8:56:ed:bb:06:e7:  
af:73:d4:29:76:bc:63:f6:2e:d1:00:51:bf:0d:db:64:25:4d:  
c5:e8:b1:1e:bd:4e:ef:5b:7a:a0:92:df:10:79:ba:41:25:d0:  
bf:e7

## 4.18.3. C509 Type 3 Certificate

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

Plain hex (307 bytes):

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

Annotated hex:

- \* See the annotated hex for the C509 type 2 certificate in Section 4.18.4. The only differences are the certificate type, the signature value, and the key identifiers.

#### 4.18.4. 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]. certificateSerialNumber=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=modulus=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

```

#### 4.19. RSASSA-PSS With SHA-384

- \* Self-signed certificate
- \* Signature algorithm: rsassa-pss-with-sha384

##### 4.19.1. Private Key

See Section 3.1.1.

##### 4.19.2. X.509 Certificate

PEM content (575 bytes):

-----BEGIN CERTIFICATE-----

MIICozCCAXCgAwIBAgICEjQwQQYJKoZIhvcNAQEKMDsgDzANBgglghkgBZQMEAgIF  
AKEcMBoGCSqGSib3DQEBCDANBgglghkgBZQMEAgIFAKIDAgEwMCUxIzAhBgNVBAMM  
GnNlbGZzaWduLXJzYXNzYS1wc3Mtc2hhMzg0MB4XDTI1MDEwMjAwMDAwMFoXDTI2  
MDEwMjAwMDAwMFowJTEjMCEGA1UEAwac2VsZnNpZ24tcnNhcnNhLXBzcy1zaGEz  
ODQwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALgJL28EcmqSHPqy0xOunS8B  
x85GX6t9pix6XHP6zl/7ovHdgKka3EM5nPyiInm4miZIEOW5JrteDT9yenY+FgE/  
ifj+rFnQ+9leiwxSgn5UkPE7hMNjTonG0XMa5fGmD4jtEY0IDhqyyqUy0GwvfSoI  
dN7k5rblcoP2R42vQlPbAgMBAAGjEjAQMA4GA1UdDwEB/wQEAwIHgDBBBgkqhkiG  
9w0BAQowNKAPMA0GCWCGSAFlAwQCAgUAoRwwGgYJKoZIhvcNAQEIIMA0GCWCGSAFl  
AwQCAgUAogMCATADgYEAqVzA6vSrfxLlxmScZDh63L2urQ7spjsiVkw6EQFEZvUT  
eJBARUoQh+skNokj0K/ThgT0Ivh2hFgrvWx69/t4h9JAy2OMGj3sAHGH8HlgsqG4  
glCKKGyhsXJqPEtOSAilslD7s5zI1xhmToKQ5ZqZVkXSSph5+rZkwKjRO67tv64=  
-----END CERTIFICATE-----

Textual Representation:

## Certificate:

Version: v3 (2)

Serial Number:

12:34

Issuer: CN=selfsign-rsassa-pss-sha384

Validity:

Not Before: Thu Jan 02 01:00:00 CET 2025

Not After : Fri Jan 02 01:00:00 CET 2026

Subject: CN=selfsign-rsassa-pss-sha384

Subject Public Key Info:

Public Key Algorithm: 1.2.840.113549.1.1.1

Pub:

30:81:89:02:81:81:00:b8:09:2f:6f:04:72:6a:92:1c:fa:b2:  
d3:13:ae:9d:2f:01:c7:ce:46:5f:ab:7d:a6:2c:7a:5c:73:fa:  
ce:5f:fb:a2:f1:dd:80:a2:9a:dc:43:39:9c:fc:a2:22:79:b8:  
9a:26:48:10:e5:b9:26:bb:5e:0d:3f:72:7a:76:3e:16:01:3f:  
89:f8:fe:ac:59:d0:fb:dd:5e:8b:0c:52:82:7e:54:90:f1:3b:  
84:c3:63:4e:89:c6:d1:73:1a:e5:f1:a6:0f:88:ed:11:8d:08:  
0e:1a:b2:ca:a5:32:d0:6c:2f:7d:2a:08:74:de:e4:e6:b6:e5:  
72:83:f6:47:8d:af:42:53:db:02:03:01:00:01

X509v3 extensions:

X509v3 keyUsage: critical

digitalSignature

Signature Algorithm: SHA384WITHRSAANDMGF1

Signature Value:

a9:5c:c0:ea:f4:ab:7f:12:e5:c6:64:9c:64:38:7a:dc:bd:ae:  
ad:0e:ec:a6:3b:22:56:45:ba:11:01:44:66:f5:13:78:90:40:  
ad:4a:10:87:eb:24:36:89:23:d0:af:d3:86:04:f4:22:f8:76:  
84:58:2b:bd:6c:7a:f7:fb:78:87:d2:40:cb:63:8c:1a:3d:ec:  
00:71:87:f0:79:60:b2:a1:b8:82:50:8a:28:6c:a1:b1:72:6a:  
3c:4b:4e:48:08:a5:b2:50:fb:b3:9c:c8:d7:18:66:4e:82:90:  
e5:9a:99:56:45:d2:4a:98:79:fa:b6:64:c0:a8:d1:3b:ae:ed:  
bf:ae

## 4.19.3. C509 Type 3 Certificate

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

Plain hex (307 bytes):

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

Annotated hex:

- \* See the annotated hex for the C509 type 2 certificate in Section 4.19.4. The only differences are the certificate type, the signature value, and the key identifiers.

#### 4.19.4. 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]. certificateSerialNumber=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=modulus=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
```

#### 4.20. RSASSA-PSS With SHA-512

- \* Self-signed certificate
- \* RSA public key with 1536-bit modulus
- \* Signature algorithm: rsassa-pss-with-sha512

##### 4.20.1. Private Key

-----BEGIN PRIVATE KEY-----

```
MIIDlgIBADANBgkqhkiG9w0BAQEFAASCA4AwggN8AgEAAoHBALURcpGG7cAbIzXs
fkarHPOzH7jUYTPONQWI79he0IdlaLe+AGzjUnq6ZDobD4+l7FQCIPYwRCz84wUI
BMsD+pnlvD+NSLPuqUtCDCb43se3joWAp54prqDcm9xZc/idmz236LvrC/01fOcQ
2e855Ktii4YShduQk58NL9AdjpvJcXz0xOQvsX3MUixCqfoACwX/+6niTuZLmRwe
AYJKnVr9w36hHIGvKh+ok9WJQK19TbYfjcaIxIpobEWxBlym0wIDAQABAoHAGnwr
BXVhPmnZxyVivT6B6sr8ggpyuLivZxgGI+COi6zThJjisrViQaMU+QOEowQ9TXZ4
fP53YnCP0RMWBw9rGcARvpfZx+lKKGtzSpo06tNYdleqbPH3jKkS6plyX18cxXKv
IXDGNeaHkrMAZUrFnyAdp84N4py6ilwe4GFSXoXsY+hUFqf2ndLnrdbtutorPOSb
OoAkSha26343TA4KbWSSjzIBdFrevSdVJKPhyXTMM7kzl8rT5ZVq6A5FxkeJAmEA
8k17eXQyp6rwXCngMvqilyd6FPiox7R37/idIhWhlByI4kTvnYphezUZnT/4RNY2
gGfwvtkU72CNx3/G2VH+IU85UqnWjleSVxt87bW/XLcURC4qRMOJB9G6Kmsodz6Z
AmEAv03NHU5Q+DtA0quYuttBDJYzatVELoR0DINO9uU17b6kpOeVrHHDqrnKaUKK
NSw7MU2jjGxUlDYblX/CfRfBgI26jefCDHRCJNBdK7XDEobcuWiR3N5G3v5RALyP
71BLAmAlTWg5Op+eFNOVYrzoWgyEdfG8RUTyIaLGsTu5XXBIP0Srfvjy6MnQzK
c/UYP4sLylHCmhy4DKwTWKgEhJ2n2f70FLbs1YFBY4A+Pdk3P1/ViyEPgOaDcAH
btVTDhkCYQC+HmjpyS/TkreCZszbbsi/5Inm81nWTQYz5U9VqTe/hcaEqC6keU82
3XuejmViILOw7ozKImMQBJH3SkgUGWqLosSTAK9lxyhxA66EorFj0qmLjbPgZ/rQ
5LfF3p/A+u8CYHb/ZTlM+RxAgAJ7bsxrUKJrkM4yRz7YXNcXZH4N6A+s4HzY1+Y/
aKaI5NsOmVR3Gr2OzpxQwALgD+Xo6hzyBPQ2gbozBA2VQ38zwt3M4dU6clFcc9R1
q1jQfu4/jlhEEg==
```

-----END PRIVATE KEY-----

#### 4.20.2. X.509 Certificate

PEM content (703 bytes):

-----BEGIN CERTIFICATE-----

```
MIICuzCCAbCgAwIBAgICEjQwQQYJKoZIhvcNAQEKMDsgDzANBgglghkgBZQMEAgMF
AKEcMBoGCSqGSib3DQEBCDANBgglghkgBZQMEAgMFAKIDAgFAMCUxIzAhBgNVBAMM
GnNlbGZzaWduLXJzYXNzYS1wc3Mtc2hhNTEyMB4XDTE1MDEwMjAwMDAwMFoXDTE2
MDEwMjAwMDAwMFowJTEjMCEGA1UEAwWac2VsZnNpZ24tcnNhcnNhLXBzcylzaGE1
MTIwgd8wDQYJKoZIhvcNAQEBBQADgcmAMIHJAoHBALURcpGG7cAbIzXsfkarHPOz
H7jUYTPONQWI79he0IdlaLe+AGzjUnq6ZDobD4+l7FQCIPYwRCz84wUIBMsD+pnl
vD+NSLPuqUtCDCb43se3joWAp54prqDcm9xZc/idmz236LvrC/01fOcQ2e855Kti
i4YShduQk58NL9AdjpvJcXz0xOQvsX3MUixCqfoACwX/+6niTuZLmRweAYJKnVr9
w36hHIGvKh+ok9WJQK19TbYfjcaIxIpobEWxBlym0wIDAQABoxIwEDAObgNVHQ8B
Af8EBAMCB4AwQQYJKoZIhvcNAQEKMDsgDzANBgglghkgBZQMEAgMFAKEcMBoGCSqG
Sib3DQEBCDANBgglghkgBZQMEAgMFAKIDAgFAA4HBAColIqgyLpIBpUstLLEaPeNe
NpA9ZibWHKT+HrHFhInSWmg6SNYDrn4/XAlj/1II9nlCvq8oq2HnHr6IUqIe6tpd
YSA5sNiAdqzSDdWRmpzpgCBzCZoxrxT3mtZ7NPqmOKYj9xRGhyrRyHB9VnEbaWxt
r2Tyr3LI6dmUsRkh+jjW31NeaLl2YAPkqsMqiXBaxiIkaYs+CwQ6UIwiY8wcdqKC
K3F9amjdTyyfZodSU8YqONqQbmZPJSuBAHxVgrumyQ==
```

-----END CERTIFICATE-----

Textual Representation:

## Certificate:

Version: v3 (2)

Serial Number:

12:34

Issuer: CN=selfsign-rsassa-pss-sha512

Validity:

Not Before: Thu Jan 02 01:00:00 CET 2025

Not After : Fri Jan 02 01:00:00 CET 2026

Subject: CN=selfsign-rsassa-pss-sha512

Subject Public Key Info:

Public Key Algorithm: 1.2.840.113549.1.1.1

Pub:

30:81:c9:02:81:c1:00:b5:11:72:91:86:ed:c0:1b:23:35:ec:  
7e:46:ab:1c:f3:b3:1f:b8:d4:61:33:ce:35:05:88:ef:d8:5e:  
d0:87:65:68:b7:be:00:6c:e3:52:7a:ba:64:3a:1b:0f:8f:a5:  
ec:54:02:22:96:30:44:2c:fc:e3:05:08:04:cb:03:fa:99:e5:  
bc:3f:8d:48:b3:ee:a9:4b:42:0c:26:f8:de:c7:b7:8e:85:80:  
a7:9e:29:ae:a0:dc:9b:dc:59:73:f8:9d:9b:3d:b7:e8:bb:eb:  
0b:fd:35:7c:e7:10:d9:ef:39:e4:ab:62:8b:86:12:85:db:90:  
93:9f:0d:2f:d0:1d:8e:9b:c9:71:7c:f4:c4:e4:2f:b1:7d:cc:  
52:2c:42:a9:fa:00:0b:05:ff:fb:a9:e2:4e:e6:4b:99:1c:1e:  
01:82:4a:9d:5a:fd:c3:7e:a1:1c:81:af:2a:1f:a8:2b:d5:89:  
40:ad:7d:4d:b6:1f:8d:c6:88:c4:8a:68:6c:45:b1:06:56:26:  
d3:02:03:01:00:01

X509v3 extensions:

X509v3 keyUsage: critical

digitalSignature

Signature Algorithm: SHA512WITHRSAANDMGF1

Signature Value:

2a:25:22:a8:32:2e:92:01:a5:4b:2d:2c:b1:1a:3d:e3:5e:36:  
90:3d:66:26:d6:1c:a4:fe:1e:b1:c5:84:83:6c:5a:68:3a:48:  
d6:03:ae:7e:3f:5c:0d:63:ff:52:08:f6:79:42:be:af:28:ab:  
61:e7:1e:be:88:52:a2:1e:ea:da:5d:61:20:39:b0:d8:80:76:  
ac:d2:0d:d5:91:9a:9c:e9:18:20:73:09:9a:31:af:14:f7:9a:  
d6:7b:34:fa:a6:38:a6:23:f7:14:46:87:2a:d1:c8:70:7d:56:  
71:1b:69:65:ed:af:64:f2:af:72:c8:e9:d9:94:b1:19:21:fa:  
38:d6:df:53:5e:68:b9:76:60:03:e4:aa:c3:2a:89:70:5a:c6:  
22:24:69:8b:3e:0b:04:3a:50:8c:22:cb:cc:1c:76:a2:82:2b:  
71:7d:68:c8:dd:4f:2c:9f:64:e7:52:53:c6:2a:38:da:90:6e:  
66:4f:25:2b:81:00:7c:55:82:bb:a6:c9

## 4.20.3. C509 Type 3 Certificate

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

Plain hex (435 bytes):

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

Annotated hex:

- \* See the annotated hex for the C509 type 2 certificate in Section 4.20.4. The only differences are the certificate type, the signature value, and the key identifiers.

#### 4.20.4. 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]. certificateSerialNumber=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=modulus=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

```

#### 4.21. RSASSA-PSS With SHAKE128

- \* Self-signed certificate
- \* Signature algorithm: rsassa-pss-with-shake128

##### 4.21.1. Private Key

See Section 3.1.1.

##### 4.21.2. X.509 Certificate

PEM content (469 bytes):

-----BEGIN CERTIFICATE-----

```
MIIB0TCCAT2gAwIBAgICEjQwCgYIKwYBBQUHbH4wJzElMCMGA1UEAwcc2VsZnNp
Z24tcnNhc3NhLXBzcylzaGFrZTEyODAEfw0yNTAxMDIwMDAwMDBaFw0yNjAxMDIw
MDAwMDBaMCcxJTAjBgNVBAMMHhNlbGZzaWduLXJzYXNzYS1wc3Mtc2hha2UxMjgw
gZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALgJL28EcmqSHPqy0xOunS8Bx85G
X6t9pix6XHP6zl/7ovHdgKKA3EM5nPyiInm4miZIEOW5JrteDT9yenY+FgE/ifj+
rFnQ+9leiwxSgn5UkPE7hMNjTonG0XMa5fGmD4jtEY0IDhqqyyqUy0GwvfSoIdN7k
5rblcoP2R42vQlPbAgMBAAGjEjAQM4GA1UdDwEB/wQEAwIHgDAKBggrBgEFBQcG
HgOBgQByM9xppigNp+i9m2mNiHR93BfwLhn0bn9889MUT+khw3LvDPUWnbqUVAj8
DwAFBzSHsZlDFilgdKEH69Ruu/+fij6pDCjoMyCset+RWZwOWdyP2bHx/JWncxjl
5lAouomFNeD+ixv2eI/sJfia0nGaVwOJmzrs5cC3wYlMzlW3GQ==
```

-----END CERTIFICATE-----

Textual Representation:

Certificate:

Version: v3 (2)

Serial Number:

12:34

Issuer: CN=selfsign-rsassa-pss-shake128

Validity:

Not Before: Thu Jan 02 01:00:00 CET 2025

Not After : Fri Jan 02 01:00:00 CET 2026

Subject: CN=selfsign-rsassa-pss-shake128

Subject Public Key Info:

Public Key Algorithm: 1.2.840.113549.1.1.1

Pub:

```
30:81:89:02:81:81:00:b8:09:2f:6f:04:72:6a:92:1c:fa:b2:
d3:13:ae:9d:2f:01:c7:ce:46:5f:ab:7d:a6:2c:7a:5c:73:fa:
ce:5f:fb:a2:f1:dd:80:a2:9a:dc:43:39:9c:fc:a2:22:79:b8:
9a:26:48:10:e5:b9:26:bb:5e:0d:3f:72:7a:76:3e:16:01:3f:
89:f8:fe:ac:59:d0:fb:dd:5e:8b:0c:52:82:7e:54:90:f1:3b:
84:c3:63:4e:89:c6:d1:73:1a:e5:f1:a6:0f:88:ed:11:8d:08:
0e:1a:b2:ca:a5:32:d0:6c:2f:7d:2a:08:74:de:e4:e6:b6:e5:
72:83:f6:47:8d:af:42:53:db:02:03:01:00:01
```

X509v3 extensions:

X509v3 keyUsage: critical

digitalSignature

Signature Algorithm: SHAKE128WITHRSAPSS

Signature Value:

```
72:33:dc:69:a6:28:0d:a7:e8:bd:9b:69:8d:88:74:7d:dc:17:
f0:2e:19:f4:6e:7f:7c:f3:d3:14:b7:e9:21:c3:72:ef:0c:f5:
16:9d:ba:94:54:08:fc:0f:00:05:07:34:87:b1:99:43:14:8d:
60:76:41:07:eb:d4:6e:bb:ff:9f:8a:3e:a9:0c:28:e8:33:20:
ac:7a:df:91:59:9c:0e:59:dc:8f:d9:b1:f1:fc:95:a7:73:18:
f5:e6:50:28:ba:89:85:35:e0:fe:8b:1b:f6:78:8f:ec:25:f8:
80:d2:71:9a:57:03:89:9b:3a:ec:e5:c0:b7:c1:8d:4c:ce:55:
b7:19
```

## 4.21.3. C509 Type 3 Certificate

- \* C509 type 3 certificate converted from the X.509 certificate in Section 4.21.2.

Plain hex (309 bytes):

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

Annotated hex:

- \* See the annotated hex for the C509 type 2 certificate in Section 4.21.4. The only differences are the certificate type, the signature value, and the key identifiers.

## 4.21.4. 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]. certificateSerialNumber=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=modulus=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

```

#### 4.22. RSASSA-PSS With SHAKE256

- \* Self-signed certificate
- \* Signature algorithm: rsassa-pss-with-shake256

##### 4.22.1. Private Key

See Section 4.20.1.

##### 4.22.2. X.509 Certificate

PEM content (597 bytes):

-----BEGIN CERTIFICATE-----

MIICUTCCAX2gAwIBAgICEjQwCgYIKwYBBQUH8wJzElMCMGA1UEAwcc2VsZnNp  
Z24tcnNhc3NhLXBzcy1zaGFrZTI1NjAeFw0yNTAxMDIwMDAwMDBaFw0yNjAxMDIw  
MDAwMDBaMCcxJTAjBgNVBAMMHhNlbGZzaWduLXJzYXNzYS1wc3Mtc2hha2UyNTYw  
gd8wDQYJKoZIhvcNAQEBBQADgcm0AMIHJAoHBALURcpGG7cAbIzXsfkarHP0zh7jU  
YTPONQWI79he0IdlaLe+AGzjUnq6ZDobD4+l7FQCIPYwRCz84wUIBMsD+pnlvD+N  
SLPuqUtCDCb43se3joWAp54prqDcm9xZc/idmz236LvrC/01fOcQ2e855Ktii4YS  
hduQk58NL9AdjpvJcXz0xOQvsX3MUixCqfoACwX/+6niTuZLmRweAYJKnVr9w36h  
HIGvKh+oK9WJQKl9TbYfjcaIxIpobEWxBLYm0wIDAQABoxIwEDAObgNVHQ8BAf8E  
BAMCB4AwCgYIKwYBBQUH8wDgcEAjurY2mbPMZ41E99aj8wWiiQhOvUIfCaGVyTW  
sYWSkNvvtn/SuszOwwD3u4GCIH7fP66LRYWthFw/3ZTpT82lqdJSfrJelBnZ7a0r  
aarrQN1eJEdJNpeF7GdJinsRXUzgDpVCYifjiBnufr3gE3Eygss0/Pr1Q/XvQ/OK  
nnCj+vQQDSOXCKeuTHGZ9cgc9kczlvP3MZmg6OLZ2KgtDgFzRJCT39JeD3p3lyn7  
j/mfBk9ZxL3vWY2gR5eDwgXvIdmK

-----END CERTIFICATE-----

Textual Representation:

## Certificate:

Version: v3 (2)

Serial Number:

12:34

Issuer: CN=selfsign-rsassa-pss-shake256

Validity:

Not Before: Thu Jan 02 01:00:00 CET 2025

Not After : Fri Jan 02 01:00:00 CET 2026

Subject: CN=selfsign-rsassa-pss-shake256

Subject Public Key Info:

Public Key Algorithm: 1.2.840.113549.1.1.1

Pub:

```
30:81:c9:02:81:c1:00:b5:11:72:91:86:ed:c0:1b:23:35:ec:
7e:46:ab:1c:f3:b3:1f:b8:d4:61:33:ce:35:05:88:ef:d8:5e:
d0:87:65:68:b7:be:00:6c:e3:52:7a:ba:64:3a:1b:0f:8f:a5:
ec:54:02:22:96:30:44:2c:fc:e3:05:08:04:cb:03:fa:99:e5:
bc:3f:8d:48:b3:ee:a9:4b:42:0c:26:f8:de:c7:b7:8e:85:80:
a7:9e:29:ae:a0:dc:9b:dc:59:73:f8:9d:9b:3d:b7:e8:bb:eb:
0b:fd:35:7c:e7:10:d9:ef:39:e4:ab:62:8b:86:12:85:db:90:
93:9f:0d:2f:d0:1d:8e:9b:c9:71:7c:f4:c4:e4:2f:b1:7d:cc:
52:2c:42:a9:fa:00:0b:05:ff:fb:a9:e2:4e:e6:4b:99:1c:1e:
01:82:4a:9d:5a:fd:c3:7e:a1:1c:81:af:2a:1f:a8:2b:d5:89:
40:ad:7d:4d:b6:1f:8d:c6:88:c4:8a:68:6c:45:b1:06:56:26:
d3:02:03:01:00:01
```

X509v3 extensions:

X509v3 keyUsage: critical

digitalSignature

Signature Algorithm: SHAKE256WITHRSAPSS

Signature Value:

```
8e:ea:d8:da:66:cf:31:9e:25:13:df:5a:8f:cc:16:8a:24:21:
3a:f5:08:7c:26:86:57:24:d6:b1:85:92:90:db:ef:b6:7f:d2:
ba:cc:ce:c3:00:f7:bb:81:82:20:7e:df:3f:ae:8b:45:85:ad:
84:5c:3f:dd:94:e9:4f:cd:a5:a9:d2:52:7e:b2:5e:d4:19:d9:
ed:ad:2b:69:aa:eb:40:dd:5e:24:47:49:36:97:85:ec:67:49:
8a:7b:11:5d:4c:e0:0e:95:42:62:27:e3:88:19:ee:7e:bd:e0:
13:71:32:82:cb:28:fc:fa:f5:43:f5:ef:43:f3:8a:9e:70:a3:
fa:f4:10:0d:23:97:0a:41:2e:4c:71:99:f5:c8:1c:f6:47:33:
96:f3:f7:31:99:a0:e8:e2:d9:d8:a8:2d:76:01:73:44:90:93:
df:d2:5e:0f:7a:77:97:29:fb:8f:f9:9f:06:4f:59:c4:bd:ef:
59:8d:a0:47:97:83:c2:05:ef:21:d9:8a
```

## 4.22.3. C509 Type 3 Certificate

- \* C509 type 3 certificate converted from the X.509 certificate in Section 4.22.2.

Plain hex (437 bytes):

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

Annotated hex:

- \* See the annotated hex for the C509 type 2 certificate in Section 4.22.4. The only differences are the certificate type, the signature value, and the key identifiers.

#### 4.22.4. C509 Type 2 Certificate

Plain hex (437 bytes):

```
02421234181EF61A6775D7001A69570A80781C73656C667369676E2D727361737361
2D7073732D7368616B653235360058C0B511729186EDC01B2335EC7E46AB1CF3B31F
B8D46133CE350588EFD85ED0876568B7BE006CE3527ABA643A1B0F8FA5EC54022296
30442CFCE3050804CB03FA99E5BC3F8D48B3EEA94B420C26F8DEC7B78E8580A79E29
AEA0DC9BDC5973F89D9B3DB7E8BBEB0BFD357CE710D9EF39E4AB628B861285DB9093
9F0D2FD01D8E9BC9717CF4C4E42FB17DCC522C42A9FA000B05FFFBA9E24EE64B991C
1E01824A9D5AFDC37EA11C81AF2A1FA82BD58940AD7D4DB61F8DC688C48A686C45B1
065626D32058C03C5A7DBA06D0918EB0397D881C60312E0668171E2644F9E30E05DC
76231AF177C8E1B460A763B31B7B869F2070602BB5749D627A7074973D4D49ADF9A2
82C506101713DD246B92AD47D2A8A914891538670F8F38F32B4C39A87C5B4FFF1DFBF
7F00A6353F199F885EA95172C334B61335A46D9DE493D2A1DB40B7CF7F39E6297D95
1CC35D459B911A591EF16511D9470C861320B6559A138D1F4AE6B4FF8E493A3B9C51
50B123FEB2FB84B5FDE60CE4FBC5FA74E4E1B9CCDAA8F2A8D4CF574263
```

Annotated hex:

```

0: 02 # [0]. certificate type=2
1: 42 # [1]. certificateSerialNumber=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=modulus=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

```

## 5. Certificates With Different RDN Attributes

### 5.1. One RDN Attribute CommonName With EUI-48

- \* Subject: a single RDN attribute, commonName, containing an EUI-48 value.

See Section 3.1.

### 5.2. One RDN Attribute CommonName With EUI-64

- \* Subject: a single RDN attribute, commonName, containing an EUI-64 value.

See Section 3.2.

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

- \* Subject: a single RDN attribute, commonName, containing an even number of lowercase hexadecimal characters.

See Section 3.3.

### 5.4. One RDN Attribute CommonName With Other Text

- \* Subject: a single RDN attribute, commonName, containing text other than an EUI-48 value, an EUI-64 value, or an even number of lowercase hexadecimal characters.

See Section 3.5.

### 5.5. Empty Subject

- \* Subject: empty.

See Section 3.6.

### 5.6. Subject With RDN Attribute Business Category

- \* Subject: includes the RDN attribute businessCategory.

See Section 3.11.

### 5.7. Subject With RDN Attribute Country

- \* Subject: includes the RDN attribute countryName.

See Section 3.8.

### 5.8. Subject With RDN Attribute Directory Management Domain Name

- \* Subject: includes the RDN attribute directoryManagementDomainName.

See Section 3.14.

### 5.9. Subject With RDN Attribute DN Qualifier

- \* Subject: includes the RDN attribute dnQualifier.

See Section 3.14.

#### 5.10. Subject With RDN Attribute Domain Component

- \* Subject: includes the RDN attribute domainComponent.

See Section 3.14.

#### 5.11. Subject With RDN Attribute Email Address

- \* Subject: includes the RDN attribute emailAddress.

See Section 3.11.

#### 5.12. Subject With RDN Attribute Generation Qualifier

- \* Subject: includes the RDN attribute generationQualifier.

See Section 3.14.

#### 5.13. Subject With RDN Attribute Given Name

- \* Subject: includes the RDN attribute givenName.

See Section 3.9.

#### 5.14. Subject With RDN Attribute Initials

- \* Subject: includes the RDN attribute initials.

See Section 3.15.

#### 5.15. Subject With RDN Attribute Jurisdiction Country

- \* Subject: includes the RDN attribute jurisdictionCountryName.

See Section 3.10.

#### 5.16. Subject With RDN Attribute Jurisdiction Locality

- \* Subject: includes the RDN attribute jurisdictionLocalityName.

See Section 3.10.

#### 5.17. Subject With RDN Attribute Jurisdiction State Or Province

- \* Subject: includes the RDN attribute jurisdictionStateOrProvinceName.

See Section 3.10.

## 5.18. Subject With RDN Attribute Locality

- \* Subject: includes the RDN attribute localityName.

See Section 3.8.

## 5.19. Subject With RDN Attribute Name

- \* Subject: includes the RDN attribute name.

See Section 3.9.

## 5.20. Subject With RDN Attribute Organization

- \* Subject: includes the RDN attribute organizationName.

See Section 3.7.

## 5.21. Subject With RDN Attribute Organizational Unit

- \* Subject: includes the RDN attribute organizationalUnitName.

See Section 3.7.

## 5.22. Subject With RDN Attribute Organization Identifier

- \* Subject: includes the RDN attribute organizationIdentifier.

See Section 3.7.

## 5.23. Subject With RDN Attribute Postal Code

- \* Subject: includes the RDN attribute postalCode.

See Section 3.8.

## 5.24. Subject With RDN Attribute Pseudonym

- \* Subject: includes the RDN attribute pseudonym.

See Section 3.15.

## 5.25. Subject With RDN Attribute Serial Number

- \* Subject: includes the RDN attribute serialNumber.

See Section 3.7.

## 5.26. Subject With RDN Attribute State

- \* Subject: includes the RDN attribute stateOrProvinceName.

See Section 3.8.

## 5.27. Subject With RDN Attribute Street

- \* Subject: includes the RDN attribute street.

See Section 3.8.

## 5.28. Subject With RDN Attribute Surname

- \* Subject: includes the RDN attribute surname.

See Section 3.9.

## 5.29. Subject With RDN Attribute Telephone Number

- \* Subject: includes the RDN attribute telephoneNumber.

See Section 3.11.

## 5.30. Subject With RDN Attribute Title

- \* Subject: includes the RDN attribute title.

See Section 3.9.

## 5.31. Subject With RDN Attribute Unstructured Address

- \* Subject: includes the RDN attribute unstructuredAddress.

See Section 3.14.

## 5.32. Subject With RDN Attribute Unstructured Name

- \* Subject: includes the RDN attribute unstructuredName.

See Section 3.14.

## 5.33. Subject With RDN Attribute User Id

- \* Subject: includes the RDN attribute userId.

See Section 3.15.

## 6. Certificates With Different Extensions

### 6.1. Empty Extensions

- \* Extensions: none

Not applicable to certificates; see Section 8.5 for examples in certification requests.

### 6.2. One Extension: Non-Critical keyUsage

- \* Extensions: a single non-critical keyUsage extension

See Section 3.1.

### 6.3. One Extension: Critical keyUsage

- \* Extensions: a single critical keyUsage extension

See Section 3.2.

### 6.4. Authority Information Access

See Section 3.12.

### 6.5. Authority Key Identifier

- \* With only the keyIdentifier field present

See Section 3.12.

- \* With all fields present

See Section 3.13.

### 6.6. ASIdentifiers And ASIdentifiers V2

- \* ASIdentifiers set to null

- \* A non-empty array of ASIdOrRange

See Section 3.8.

### 6.7. Basic Constraints

- \* CA = true and pathLenConstraint absent

See Section 3.3.

- \* CA = true and pathLenConstraint present

See Section 3.5.

- \* CA = false

See Section 3.6.

#### 6.8. Certificate Policies

See Section 3.5.

#### 6.9. CRL Distribution Points and Freshest CRL

See Section 3.13.

#### 6.10. Extended Key Usage

- \* Integer-identified usages

See Section 3.3.

- \* ~oid-identified usages

See Section 3.5.

- \* Integer-identified and ~oid-identified usages

See Section 3.6.

#### 6.11. Inhibit anyPolicy

See Section 3.5.

#### 6.12. Issuer Alternative Name

See Section 3.12.

#### 6.13. IPAddrBlocks and IPAddrBlocks V2

- \* With SAFI = null and IP Address Choice = null

- \* With SAFI = null and IP Address Choice = null

See Section 3.8.

- \* IPAddrBlocks with non-null SAFI and IntIPAddressChoice'

- \* IPAddrBlocks V2 with non-null SAFI, IntIPAddressChoice and IPAddressChoice

See Section 3.9.

#### 6.14. Name Constraints

- \* Only PermittedSubTree

See Section 3.11.

- \* Only ExcludedSubTree

See Section 3.7.

- \* Both PermittedSubTree and ExcludedSubTree

See Section 3.14.

#### 6.15. OCSP No Check

See Section 3.15.

#### 6.16. Policy Constraints

- \* Only RequireExplicitPolicy

See Section 3.11.

- \* Only InhibitPolicyMapping

See Section 3.7.

- \* Both RequireExplicitPolicy and InhibitPolicyMapping

See Section 3.14.

#### 6.17. Policy Mappings

See Section 3.10.

#### 6.18. Subject Alternative Name

See Section 3.6.

## 6.19. Subject Directory Attributes

See Section 3.10.

## 6.20. Subject Information Access

See Section 3.10.

## 6.21. Subject Key Identifier

See Section 3.3.

## 6.22. TLS Features

See Section 3.15.

## 7. X.509 Certificate With Unconvertible RDN Attributes And Extensions

- \* Common Name: text encoded in a string type other than PrintableString or UTF8String.
- \* Subject Public Key Algorithm: an EC public key with an unknown curve OID in the parameters field.
- \* ASIdentifiers: includes the rdi field.
- \* Name Constraints: includes a DirectoryName option encoded as IA5String.

## 7.1. Private Key

See Section 3.3.1.

## 7.2. X.509 Certificate

PEM content (387 bytes)

```
-----BEGIN CERTIFICATE-----
MIIBfzCCASWgAwIBAgIBATAKBggqhkJOPQQDAjAimsAwHgYDVQQDFhdBbiBJQTVT
dHJpbmcgQ29tbW9uTmFtZTAeFw0yNTAxMDIwMDAwMDBaFw0yNjAxMDIwMDAwMDBa
MCIxIDAeBgNVBAMWF0FuIElBNVN0cmcluZyBDb21tb250YW11MFowFAYHKoZIzj0C
AQYJKwYBBAGB/VkFA0IABPQTWWqHElmVtODYt777xNbtsR9hrwirMkCNT/n5B43b
qzYlr9SW1WVqIu/cPVnESCqZg2uzWPv0ynjTkWQ2yFejSzBJMBIGCCsGAQUFBwEI
BAYwBKECBQAwMwYDVR0eBCwwKqAoMCakJDAimsAwHgYDVQQDFhdBbiBJQTVTdHJp
bmcgQ29tbW9uTmFtZTAKBggqhkJOPQQDAgNIADBFAiEAiiXoqrksZuODRWWpHbC
xC9QaPXzRXYGg4vKEoi5ucIE94fU4E/kti3t2ogAd9yCSqXXodjtYjCc1GfmGF
TcMK
-----END CERTIFICATE-----
```

## Textual Representation:

## Certificate:

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 nameConstraints:

Permitted

Directory Name: CN=An IA5String CommonName

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:

e7:02:20:4f:78:7d:4e:04:fe:4b:62:de:dd:a8:80:07:7d:c9:

cb:2a:5d:7a:1d:8e:d6:23:09:cd:46:7e:61:85:4d:c3:0a

## Text representation:

## Certificate:

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 nameConstraints:

Permitted

Directory Name: CN=An IA5String CommonName

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:

e7:02:20:4f:78:7d:4e:04:fe:4b:62:de:dd:a8:80:07:7d:c9:

cb:2a:5d:7a:1d:8e:d6:23:09:cd:46:7e:61:85:4d:c3:0a

## 7.3. C509 Type 3 Certificate

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

Plain hex (256 bytes):

```
03410100F61A6775D7001A69570A80824355040358191617416E2049413553747269
6E6720436F6D6D6F6E4E616D6582472A8648CE3D02014B06092B0601040181FD5905
584104F413596A87125995B4E0D8B7BEFBC4D6EDB11F61AF08AB32408D4FF9F9078D
DBAB3635AFD496D5656A22EFDC3D59C4482A99836BB358FBF4CA78D3930436C85784
482B06010505070108463004A1020500181A828204824355040358191617416E2049
4135537472696E6720436F6D6D6F6E4E616D65F658408A25E8AABBA4B19B8E0D1596
A476C2C42F5068F5F3457606806E2F284A22E6E74F787D4E04FE4B62DEDDA880077D
C9CB2A5D7A1D8ED62309CD467E61854DC30A
```

Annotated hex:

```
0: 03 # [0]. certificate type=3
1: 41 # [1]. certificateSerialNumber=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: 4B # parameters=byte[11]
57: 06092B0601040181FD5905
68: 58 41 # [8]. subject public key=byte[65]
70: 04F413596A87125995B4E0D8B7BEFBC4D6EDB11F61AF08AB32408D4FF9F9
100: 078DDBAB3635AFD496D5656A22EFDC3D59C4482A99836BB358FBF4CA78D3
130: 930436C857
135: 84 # [9]. extensions=array[4]
extension[0]
136: 48 # type=byte[8]:
137: 2B06010505070108 # oid: 1.3.6.1.5.5.7.1.8
(ASIdentifiers)
145: 46 # value=byte[6]
146: 3004A1020500
extension[1]
152: 18 1A # type=26: NameConstraints
154: 82 # value=array[2]
155: 82 # permittedSubtrees=array[2]
GeneralName[0]
156: 04 # GeneralNameType=4: directoryName
157: 82 # GeneralNameValue=array[2], 1
attribute
attribute[0]
158: 43 # type=byte[3]:
159: 550403 # oid: 2.5.4.3 (commonName)
162: 58 19 # value=byte[25]
164: 1617416E20494135537472696E6720436F6D6D6F6E4E61
187: 6D65
189: F6 # excludedSubtrees=<null>
190: 58 40 # [10]. signature value=byte[64]
192: 8A25E8AABBA4B19B8E0D1596A476C2C42F5068F5F3457606806E2F284A22
222: E6E74F787D4E04FE4B62DEDDA880077DC9CB2A5D7A1D8ED62309CD467E61
```

252: 854DC30A

## 8. Certification Requests With Different Signature Algorithms

### 8.1. ECDSA With SHA256

- \* Signature algorithm: ecdsa-with-sha256
- \* CR attributes: one extensionRequest attribute.

#### 8.1.1. Private Key

See Section 3.3.1.

#### 8.1.2. X.509 Certification Request

PEM content (248 bytes):

```
-----BEGIN CERTIFICATE REQUEST-----
MIH1MIGcAgEAMBUxEzARBgNVBAMMCmVjZHNhLXAYNTYwWTATBgqhkhjOPQIBBggq
hkjOPQMBBwNCAAT0E1lqhXJZ1bTg2Le++8TW7bEfYa8IqzJAjU/5+QeN26s2Na/U
ltVlaiLv3DlZxEgqmYNrs1j79Mp405MENshXoCUwIwYJKoZIHvcNAQkOMRYwFDAS
BgNVHREECzAJggdhYmMuY29tMAoGCCqGSM49BAMCA0gAMEUCIQCKJeiqu6Sxm44N
FZakdsLEL1Bo9fNFDgaAbi8oSiLm5wIgMB7Y07KH0Jy95tedwnlGt0ISoyrzjtwH
IocYDepNODo=
-----END CERTIFICATE REQUEST-----
```

Text representation:

## Certificate Request:

## Data:

Version: v1 (0)

Subject: CN=ecdsa-p256

## Subject Public Key Info:

Public Key Algorithm: EC/P256

## 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:

30:45:02:21:00:8a: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:  
e7:02:20:30:1e:d8:d3:b2:87:d0:9c:bd:e6:d7:9d:c2:79:46:  
b7:42:12:a3:2a:f3:8e:dc:07:22:87:18:0d:ea:4d:38:3a

## 8.1.3. C509 Type 3 Certification Request

- \* C509 type 3 certification request converted from the X.509 certification request in Section 8.1.2.

## Plain hex (159 bytes):

03006A65636473612D7032353601584104F413596A87125995B4E0D8B7BEFBC4D6ED  
B11F61AF08AB32408D4FF9F9078DDBAB3635AFD496D5656A22EFDC3D59C4482A9983  
6BB358FBF4CA78D3930436C85782008203676162632E636F6D58408A25E8AABBA4B1  
9B8E0D1596A476C2C42F5068F5F3457606806E2F284A22E6E7301ED8D3B287D09CBD  
E6D79DC27946B74212A32AF38EDC072287180DEA4D383A

## Annotated hex:

- \* See the annotated hex for the C509 type 2 certification request in Section 8.1.4. The only differences are the certification request type and the signature value.

## 8.1.4. C509 Type 2 Certification Request

## Plain hex (159 bytes):

```

02006A65636473612D7032353601584104F413596A87125995B4E0D8B7BEFBC4D6ED
B11F61AF08AB32408D4FF9F9078DDBAB3635AFD496D5656A22EFDC3D59C4482A9983
6BB358F4CA78D3930436C85782008203676162632E636F6D58408A25E8AABBA4B1
9B8E0D1596A476C2C42F5068F5F3457606806E2F284A22E6E7968BE4355C30FDBA65
AAC518ACAEA710B1B626623F7B6F747D0D6DD4A2808C92

```

Annotated hex:

```

0: 02 # [0]. c509CertificationRequestType=2
1: 00 # [1]. subjectSignatureAlgorithm=0:
 # ecdsa-with-sha256
2: 6A # [2]. subject=char[10]
3: 65636473612D70323536 # "ecdsa-p256"
13: 01 # [3]. subjectPublicKeyAlg=1: EC public key on
 # curve secp256r1
14: 58 41 # [4]. subject public key=EC point=byte[65]
16: 04F413596A87125995B4E0D8B7BEFBC4D6EDB11F61AF08AB32408D4FF9F9
46: 078DDBAB3635AFD496D5656A22EFDC3D59C4482A99836BB358F4CA78D3
76: 930436C857
81: 82 # [5]. attributes=array[2]
 # attribute[0]
82: 00 # type=0: ExtensionRequest
83: 82 # extensions=array[2]
 # extension[0]
84: 03 # type=3: SubjectAlternativeName
85: 67 # DNS, value=char[7]
86: 6162632E636F6D # "abc.com"
93: 58 40 # [6]. signature value=byte[64]
95: 8A25E8AABBA4B19B8E0D1596A476C2C42F5068F5F3457606806E2F284A22
125: E6E7968BE4355C30FDBA65AAC518ACAEA710B1B626623F7B6F747D0D6DD4
155: A2808C92

```

## 8.2. ECDSA With SHA384

- \* Signature algorithm: ecdsa-with-sha384
- \* CR attributes: one challengePassword attribute with a PrintableString value.

### 8.2.1. Private Key

See Section 3.5.1.

### 8.2.2. X.509 Certification Request

PEM content (300 bytes):

```

-----BEGIN CERTIFICATE REQUEST-----
MIIBKDCBsAIBADAVMRMwEQYDVQDDApLY2RzYS1wMzg0MHYwEAYHKOZIZj0CAQYF
K4EEACIDYgAE3Wdi8DWJlFE3Ky/ptSqDFK0Q4sQ2PFpYSeKW/lGqub/QOrA40zQY
oLzYMoCroL2RBAFxZcBITTrVBCErJ/MiJ5O6HC1+KLGPa5BTeGXVb4nihdeBA1K
TBoO5G6SSlwpOBwwGgYJKoZIhvcNAQkHMQ0TC215IHBhc3N3b3JkMAoGCCqGSM49
BAMDA2cAMGQCMR+telJ4fZTbio/O13xwS2brvRA37xCvUXTH0s/2r36nWhahFgt
mLGyR0IQ8ceF2gIwY8kdAQd6yDL0bKUsrMs6bBlgvdqBMFj7a4Za0riFSStpfUUP
buBrmI16HsX89Kam
-----END CERTIFICATE REQUEST-----

```

Text representation:

Certificate Request:

Data:

Version: v1 (0)

Subject: CN=ecdsa-p384

Subject Public Key Info:

Public Key Algorithm: EC/P384

Pub:

```

04:dd:67:62:f0:35:89:94:51:37:2b:2f:e9:b5:2a:83:14:ad:
10:e2:c4:36:3c:5a:58:49:e2:96:fe:51:aa:b9:bf:d0:3a:b0:
38:d3:34:18:a0:bc:d8:32:80:ab:a0:bd:91:04:01:71:65:c0:
48:b5:34:6b:54:10:9e:44:9f:cc:88:9e:4e:e8:70:b5:f8:a2:
c6:3d:ae:41:4d:e1:97:55:be:27:8a:17:5e:04:0d:4a:4c:1a:
0e:e4:6e:92:4a:5c:29

```

Attributes:

challengePassword: my password

Signature Algorithm: SHA384WITHECDSA

Signature Value:

```

30:64:02:30:34:7e:b5:ed:49:e1:f6:53:6e:2a:3f:3b:5d:f1:
c1:2d:9b:ae:f4:40:df:bc:42:bd:45:d3:1f:4b:3f:da:bd:fa:
9d:68:5a:84:58:2d:98:b1:b2:47:42:10:f1:c7:85:da:02:30:
63:c9:1d:01:07:7a:c8:32:f4:6c:a5:2c:ac:cb:3a:6c:1d:60:
bd:da:81:30:58:fb:6b:86:5a:d2:b8:85:49:2b:69:7d:45:0f:
6e:e0:6b:98:8d:7a:1e:c5:fc:f4:a6:a6

```

### 8.2.3. C509 Type 3 Certification Request

- \* C509 type 3 certification request converted from the X.509 certification request in Section 8.2.2.

Plain hex (227 bytes):

```

03016A65636473612D7033383402586104DD6762F035899451372B2FE9B52A8314AD
10E2C4363C5A5849E296FE51AAB9BFD03AB038D33418A0BCD83280ABA0BD91040171
65C048B5346B54109E449FCC889E4EE870B5F8A2C63DAE414DE19755BE278A175E04
0D4A4C1A0EE46E924A5C298201D8796B6D792070617373776F72645860347EB5ED49
E1F6536E2A3F3B5DF1C12D9BAEF440DFBC42BD45D31F4B3FDABDFA9D685A84582D98
B1B2474210F1C785DA63C91D01077AC832F46CA52CACCB3A6C1D60BDDA813058FB6B
865AD2B885492B697D450F6EE06B988D7A1EC5FCF4A6A6

```

Annotated hex:

```

0: 02 # [0]. c509CertificationRequestType=2
1: 01 # [1]. subjectSignatureAlgorithm=1:
 # ecdsa-with-sha384
2: 6A # [2]. subject=char[10]
3: 65636473612D70333834 # "ecdsa-p384"
13: 02 # [3]. subjectPublicKeyAlg=2: EC public key on
 # curve secp384r1
14: 58 61 # [4]. subject public key=EC point=byte[97]
16: 04DD6762F035899451372B2FE9B52A8314AD10E2C4363C5A5849E296FE51
46: AAB9BFD03AB038D33418A0BCD83280ABA0BD9104017165C048B5346B5410
76: 9E449FCC889E4EE870B5F8A2C63DAE414DE19755BE278A175E040D4A4C1A
106: 0EE46E924A5C29
113: 82 # [5]. attributes=array[2]
 # attribute[0]
114: 01 # type=1: ChallengePassword
115: D8 79 # tag=121: alternative 0, PRINTABLE STRING
117: 6B # char[11]
118: 6D792070617373776F7264 # "my password"
129: 58 60 # [6]. signature value=byte[96]
131: 347EB5ED49E1F6536E2A3F3B5DF1C12D9BAEF440DFBC42BD45D31F4B3FDA
161: BDF9A9D685A84582D98B1B2474210F1C785DA27C5D36FFA887A38BACBD8D7
191: D241E770B513B034E32ACB43D5AF979E122E2FAB403D4D30DF44D077C5A0
221: 5E1E07981567

```

#### 8.2.4. C509 Type 2 Certification Request

A PrintableString challengePassword value is not supported in a type 2 certification request.

#### 8.3. ECDH PoP With SHA-256 And HMAC-SHA256

- \* Signature algorithm: sa-ecdhPop-sha256-hmac-sha256
- \* Signature value: only the hashValue field is present.
- \* CR attributes: one challengePassword attribute with a UTF8String value.

### 8.3.1. Private Key

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

### 8.3.2. X.509 Certification Request

- \* The peer private key and certificate are given in Section 3.3.1 and Section 3.3.2.

PEM content (206 bytes):

```
-----BEGIN CERTIFICATE REQUEST-----
MIHLMIGVAgEAMBCxFTATBgNVBAMMDGRoc2lnLXNoYTI1NjBZMBMGByqGSM49AgEG
CCqGSM49AwEHA0IABMTUozeP7JAAXLsNPq8TCbSCkprlZhSvJqnyLbg8TzR3sLqX
Et+CE3Sfky1979+zKmxD3wlxXQDke+BRnSDksxSgHDAaBgkqhkiG9w0BCQcxDQwL
bXkgcGFzc3dvcmQwCgYIKwYBBQUHBoDJQAwIgQgCKW6hVQ4LZIOFihpg9OcVWST
6wIOKgvdwZd4lBNtB9k=
-----END CERTIFICATE REQUEST-----
```

Text representation:

Certificate Request:

Data:

Version: v1 (0)

Subject: CN=dhsig-sha256

Subject Public Key Info:

Public Key Algorithm: EC/P256

Pub:

04:c4:d4:a3:37:8f:ec:90:00:5c:bb:0d:3e:af:13:09:b4:82:

92:9a:f5:66:14:af:26:a9:f2:2d:b8:3c:4f:34:77:b0:ba:97:

12:df:82:13:74:9f:91:8d:7d:ef:df:b3:2a:6c:43:df:09:71:

5d:00:e4:7b:e0:51:9d:20:e4:b3:14

Attributes:

challengePassword: my password

Signature Algorithm: sa-ecdhPop-sha256-hmac-sha256

Signature Value:

Hash Value:

08:a5:ba:85:54:38:2d:92:0e:16:28:69:83:d3:9c:55:64:93:

eb:02:0e:2a:0b:dd:c1:97:78:94:13:6d:07:d9

### 8.3.3. C509 Type 3 Certification Request

- \* C509 type 3 certification request converted from the X.509 certification request in Section 8.3.2.

Plain hex (131 bytes):

```
030E6C64687369672D73686132353601584104C4D4A3378FEC90005CBB0D3EAF1309
B482929AF56614AF26A9F22DB83C4F3477B0BA9712DF8213749F918D7DEFDFB32A6C
43DF09715D00E47BE0519D20E4B31482016B6D792070617373776F7264582008A5BA
8554382D920E16286983D39C556493EB020E2A0BDDC1977894136D07D9
```

Annotated hex:

- \* See the annotated hex for the C509 type 2 certification request in Section 8.3.4. The only differences are the certification request type and the signature value.

#### 8.3.4. C509 Type 2 Certification Request

- \* The peer private key and certificate are given in Section 3.3.1 and Section 3.3.4.

Plain hex (131 bytes):

```
020E6C64687369672D73686132353601584104C4D4A3378FEC90005CBB0D3EAF1309
B482929AF56614AF26A9F22DB83C4F3477B0BA9712DF8213749F918D7DEFDFB32A6C
43DF09715D00E47BE0519D20E4B31482016B6D792070617373776F726458202C237A
82D11BD92EF29A69EA046128BF2CFF2F07ABF2499E966D81D712E4637C
```

Annotated hex:

```
0: 02 # [0]. c509CertificationRequestType=2
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 on
 # curve secp256r1
16: 58 41 # [4]. subject public key=EC point=byte[65]
18: 04C4D4A3378FEC90005CBB0D3EAF1309B482929AF56614AF26A9F22DB83C
48: 4F3477B0BA9712DF8213749F918D7DEFDFB32A6C43DF09715D00E47BE051
78: 9D20E4B314
83: 82 # [5]. attributes=array[2]
 # attribute[0]
84: 01 # type=1: ChallengePassword
85: 6B # char[11]
86: 6D792070617373776F7264 # "my password"
97: 58 20 # [6]. signature
 # value=DhSigStatic.hashValue=byte[32]
99: 2C237A82D11BD92EF29A69EA046128BF2CFF2F07ABF2499E966D81D712E4
129: 637C
```

## 8.4. ECDH PoP With SHA-384 And HMAC-SHA384

- \* Signature algorithm: sa-ecdhPop-sha384-hmac-sha384
- \* Signature value: all fields are present.
- \* CR attributes: none.

## 8.4.1. Private Key

```
-----BEGIN PRIVATE KEY-----
ME4CAQAwEAYHKoZIzj0CAQYFK4EEACIENzA1AgEBBDBUbyPmsdFTjH5242lnccrR
+S9hKNFLUk7CGvyvn2qPBrvxTwFk0g+y5Kb0yGm9mFc=
-----END PRIVATE KEY-----
```

## 8.4.2. X.509 Certification Request

- \* The peer private key and certificate are given in Section 3.5.1 and Section 3.5.2.

PEM content (261 bytes):

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBATCBlgIBADAXMRUwEwYDVQQDDAxkaHNpZy1zaGEzODQwdjAQBgcqhkjOPQIB
BgUrgQQAIgNiAAQKxeNs56ZnUpvRp6BZmvKELxvkk9P+0gApVXSg2LvxoQfBSIrP
CZoyRp67HFpzLWnC+TVnIoahKc6IeEx72NBX1j4l/dDyjdWbpsWMJXHYxoOIaqaj
ift9JLlIm5l0N3WgADAKBggrBgEFBQcGGwNaADBXMCMwHTEbMBkGA1UEAwSc2Vs
ZnNpZ24tc2VjcDM4NHlxAQISNAQwD2dT3Gjb9kiZ3hf59DgzhB/2WonQkMZMcUY
EKaPr3weGTBEiMk+FCxXLRBT001G
-----END CERTIFICATE REQUEST-----
```

Text representation:

## Certificate Request:

## Data:

Version: v1 (0)

Subject: CN=dhsig-sha384

Subject Public Key Info:

Public Key Algorithm: EC/P384

Pub:

```
04:0a:c5:e3:6c:e7:a6:67:52:9b:d1:a7:a0:59:9a:f2:84:2f:
1b:e4:93:d3:fe:d2:00:29:55:74:a0:d8:bb:f1:a1:07:c1:48:
8a:cf:09:9a:32:46:9e:bb:1c:5a:73:2d:69:c2:f9:35:67:22:
86:87:29:ce:88:78:4c:7b:d8:d0:57:d6:3e:25:fd:d0:f2:8c:
35:9b:a6:c5:8c:25:71:d8:c6:83:88:6a:a6:a3:89:fb:7d:24:
b9:62:9b:99:74:37:75
```

Attributes:

Signature Algorithm: sa-ecdhPop-sha384-hmac-sha384

Signature Value:

Issuer: CN=selfsign-secp384r1

Serial Number:

12:34

Hash Value:

```
0f:67:53:b3:71:a3:6f:d9:22:67:78:45:e7:d0:e0:ce:10:7f:
d9:6a:27:42:43:19:31:c5:18:10:a6:8f:af:7c:1e:19:30:44:
88:c9:3e:14:2c:57:2d:10:53:d0:ed:46
```

## 8.4.3. C509 Type 3 Certification Request

- \* C509 type 3 certification request converted from the X.509 certification request in Section 8.4.2.

Plain hex (189 bytes):

```
030F6C64687369672D736861333834025861040AC5E36CE7A667529BD1A7A0599AF2
842F1BE493D3FED200295574A0D8BBF1A107C1488ACF099A32469EBB1C5A732D69C2
F9356722868729CE88784C7BD8D057D63E25FDD0F28C359BA6C58C2571D8C683886A
A6A389FB7D24B9629B9974377580837273656C667369676E2D736563703338347231
42123458300F6753B371A36FD922677845E7D0E0CE107FD96A2742431931C51810A6
8FAF7C1E19304488C93E142C572D1053D0ED46
```

Annotated hex:

- \* See the annotated hex for the C509 type 2 certification request in Section 8.4.4. The only differences are the certification request type and the signature value.

## 8.4.4. C509 Type 2 Certification Request

- \* The peer private key and certificate are given in Section 3.5.1 and Section 3.5.4.

Plain hex (189 bytes):

```
020F6C64687369672D736861333834025861040AC5E36CE7A667529BD1A7A0599AF2
842F1BE493D3FED200295574A0D8BBF1A107C1488ACF099A32469EBB1C5A732D69C2
F9356722868729CE88784C7BD8D057D63E25FDD0F28C359BA6C58C2571D8C683886A
A6A389FB7D24B9629B9974377580837273656C667369676E2D736563703338347231
42123458300C5E7EADF9C902D6ED67ACBEF42EFD563A0D6478182726571B3D9F04DE
FD2693ED3CDF0AEEF102AF104F1871BC9DEB75
```

Annotated hex:

```
0: 02 # [0]. c509CertificationRequestType=2
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 on
 # curve secp384r1
16: 58 61 # [4]. subject public key=EC point=byte[97]
18: 040AC5E36CE7A667529BD1A7A0599AF2842F1BE493D3FED200295574A0D8
48: BBF1A107C1488ACF099A32469EBB1C5A732D69C2F9356722868729CE8878
78: 4C7BD8D057D63E25FDD0F28C359BA6C58C2571D8C683886AA6A389FB7D24
108: B9629B99743775
115: 80 # [5]. attributes=array[0]
116: 83 # [6]. signature value=DhSigStatic=array[3]
117: 72 # issuer=char[18]
118: 73656C667369676E2D73656370333834 # "selfsign-secp384"
134: 7231 # "r1"
136: 42 # certificateSerialNumber=byte[2]
137: 1234
139: 58 30 # hashCode=byte[48]
141: 0C5E7EADF9C902D6ED67ACBEF42EFD563A0D6478182726571B3D9F04DE
170: FD2693ED3CDF0AEEF102AF104F1871BC9DEB75
```

#### 8.5. ECDH PoP With SHA-512 And HMAC-SHA512

- \* Signature algorithm: sa-ecdhPop-sha512-hmac-sha512
- \* Signature value: only the hashCode field is present.
- \* CR attributes: none.

##### 8.5.1. Private Key

```

-----BEGIN PRIVATE KEY-----
MF8CAQAwEAYHKoZIzj0CAQYFK4EEACMEsDBAgEBBEGYAujVrO97/rkH82IyZSy
71Rtimax0VONomS0XClgUOA1+6U8bwhyjFiEMQsJC5mrLpJeu05Z6IGl/uwnS5It
LA==
-----END PRIVATE KEY-----

```

#### 8.5.2. X.509 Certification Request

- \* The peer private key and certificate are given in Section 3.6.1 and Section 3.6.2.

PEM content (278 bytes):

```

-----BEGIN CERTIFICATE REQUEST-----
MIIBEjCBvAIBADAXMRUwEwYDVQQDDAxkaHNpZy1zaGE1MTIwZSwEAYHKoZIzj0C
AQYFK4EEACMDgYYABAFoRTEuNgFjmmHiGcPDj768sqCrVOaYYW88gPqP9et8WCn8
TPILotzY/IQV0uf+a5KoRHQNfOpLnpJPAQ6l0Jf7jQCBOWzQvsXh2AFUdvWHzndS
5LlWKiYOyqL3CuTNL02dv0dKWJjFWj/bc27z8ftrjLbG2OSj33K2rYutzXyocWjg
36AAMaOGCCsGAQUFBwYcA0UAMEIEQM9Q4zytz9NGAX2C9cq+d+hhhxPCIZ2votIm7
57WqRA+yuIso3clDCopETMiLwfbyljYmv8UPC9P/RUFpbORYRag=
-----END CERTIFICATE REQUEST-----

```

Text representation:

Certificate Request:

Data:

Version: v1 (0)

Subject: CN=dhsig-sha512

Subject Public Key Info:

Public Key Algorithm: EC/P521

Pub:

```

04:01:68:ad:31:2e:36:01:63:9a:61:e2:19:c3:c3:8f:be:bc:
b2:a0:ab:54:e6:98:61:6f:3c:80:fa:8f:f5:eb:7c:58:29:fc:
4c:f2:0b:a2:dc:d8:fc:84:15:d2:e7:fe:6b:92:a8:44:74:0d:
7c:ea:4b:9e:92:4f:01:0e:a5:d0:97:fb:8d:00:81:39:6c:d0:
be:c5:e1:d8:01:54:76:f5:87:ce:77:52:e4:bd:56:2a:26:0e:
ca:a2:f7:0a:e4:cd:2f:4d:9d:bf:47:4a:58:98:c5:5a:3f:db:
73:6e:f3:f1:fb:6b:8c:b6:c6:d8:e4:a3:df:72:b6:ad:8b:ad:
cd:7c:a8:71:68:e0:df

```

Attributes:

Signature Algorithm: sa-ecdhPop-sha512-hmac-sha512

Signature Value:

Hash Value:

```

cf:50:e3:3c:ad:cf:d3:46:01:7d:82:f5:ca:9d:fa:18:61:c4:
f0:88:67:6b:e8:b4:89:bb:e7:b5:aa:44:0f:b2:b8:8b:28:dd:
c9:43:0a:8a:44:4c:c8:8b:c1:f6:f2:d6:36:26:bf:c5:0f:0b:
d3:ff:45:41:69:6c:e4:58:44:08

```

### 8.5.3. C509 Type 3 Certification Request

- \* C509 type 3 certification request converted from the X.509 certification request in Section 8.5.2.

Plain hex (218 bytes):

```
03106C64687369672D736861353132035885040168AD312E3601639A61E219C3C38F
BEB CB2A0AB54E698616F3C80FA8FF5EB7C5829FC4CF20BA2DCD8FC8415D2E7FE6B92
A844740D7CEA4B9E924F010EA5D097FB8D0081396CD0BEC5E1D8015476F587CE7752
E4BD562A260EC AA2F70AE4CD2F4D9DBF474A5898C55A3FDB736EF3F1FB6B8CB6C6D8
E4A3DF72B6AD8BADCD7CA87168E0DF805840CF50E33CADCFD346017D82F5CA9DFA18
61C4F088676BE8B489BBE7B5AA440FB2B88B28DDC9430A8A444CC88BC1F6F2D63626
BFC50F0BD3FF4541696CE4584408
```

Annotated hex:

- \* See the annotated hex for the C509 type 2 certification request in Section 8.5.4. The only differences are the certification request type and the signature value.

### 8.5.4. C509 Type 2 Certification Request

- \* The peer private key and certificate are given in Section 3.6.1 and Section 3.6.4.

Plain hex (218 bytes):

```
02106C64687369672D736861353132035885040168AD312E3601639A61E219C3C38F
BEB CB2A0AB54E698616F3C80FA8FF5EB7C5829FC4CF20BA2DCD8FC8415D2E7FE6B92
A844740D7CEA4B9E924F010EA5D097FB8D0081396CD0BEC5E1D8015476F587CE7752
E4BD562A260EC AA2F70AE4CD2F4D9DBF474A5898C55A3FDB736EF3F1FB6B8CB6C6D8
E4A3DF72B6AD8BADCD7CA87168E0DF80584061D337C6DBF89F04E020728F37C6F42A
9B9AF25ADF51B334D1F8AF26BCB048DF3896097FA1FAEA65DC34B945C2022AA3727B
D75A75F557370250C05E9DE6B0D7
```

Annotated hex:

```

0: 02 # [0]. c509CertificationRequestType=2
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 on
 # curve secp521r1
16: 58 85 # [4]. subject public key=EC point=byte[133]
18: 040168AD312E3601639A61E219C3C38FBEB2A0AB54E698616F3C80FA8F
48: F5EB7C5829FC4CF20BA2DCD8FC8415D2E7FE6B92A844740D7CEA4B9E924F
78: 010EA5D097FB8D0081396CD0BEC5E1D8015476F587CE7752E4BD562A260E
108: CAA2F70AE4CD2F4D9DBF474A5898C55A3FDB736EF3F1FB6B8CB6C6D8E4A3
138: DF72B6AD8BADCD7CA87168E0DF
151: 80 # [5]. attributes=array[0]
152: 58 40 # [6]. signature
 # value=DhSigStatic.hashValue=byte[64]
154: 61D337C6DBF89F04E020728F37C6F42A9B9AF25ADF51B334D1F8AF26BCB0
184: 48DF3896097FA1FAEA65DC34B945C2022AA3727BD75A75F557370250C05E
214: 9DE6B0D7

```

#### 8.6. Unsigned PoP With X25519 Key

- \* Signature algorithm: unsigned
- \* CR attributes: a privateKeyPossessionStatement attribute without the cert field.

##### 8.6.1. Private Key

```

-----BEGIN PRIVATE KEY-----
MC4CAQAwBQYDK2VuBCIEIPJNe3l0Mqeqq8Fwp4DL6opcnehT4qMe0d+/4nSIVodQc
-----END PRIVATE KEY-----

```

##### 8.6.2. X.509 Certification Request

PEM content (135 bytes):

```

-----BEGIN CERTIFICATE REQUEST-----
MIGEMHMCQAQAwETEPMA0GA1UEAwGeDI1NTE5MCCowBQYDK2VuAyeAiv9Rb6xxJEFQ
5w+Sd/St9/sp9Bp6SogovUdnIvwbfiwigLzAtBgorBgEEAYGSAIBMR8wHTAbMBYx
FDASBgNVBAMMC2RlbW8gaXNzdWVyAgECMAoGCCsGAQUFBwYkAwEA
-----END CERTIFICATE REQUEST-----

```

Text representation:

## Certificate Request:

## Data:

Version: v1 (0)

Subject: CN=x25519

## Subject Public Key Info:

Public Key Algorithm: X25519

## Pub:

8a:ff:51:6f:ac:71:24:41:50:e7:0f:92:77:f4:ad:f7:fb:29:

f4:1a:7a:4a:88:28:bd:47:67:22:fc:1b:7f:08

## Attributes:

## PrivateKeyPossessionStatement:

## signer:

Issuer: CN=demo issuer

Serial Number:

02

Signature Algorithm: unsigned

Signature Value: &lt;empty&gt;

## 8.6.3. C509 Type 3 Certification Request

- \* C509 type 3 certification request converted from the X.509 certification request in Section 8.6.2.

Plain hex (63 bytes):

0305667832353531390858208AFF516FAC71244150E70F9277F4ADF7FB29F41A7A4A  
8828BD476722FC1B7F088202836B64656D6F206973737565724102F640

Annotated hex:

- \* See the annotated hex for the C509 type 2 certification request in Section 8.6.4. The only differences are the certification request type and the signature value.

## 8.6.4. C509 Type 2 Certification Request

Plain hex (63 bytes):

0205667832353531390858208AFF516FAC71244150E70F9277F4ADF7FB29F41A7A4A  
8828BD476722FC1B7F088202836B64656D6F206973737565724102F640

Annotated hex:

```

0: 02 # [0]. c509CertificationRequestType=2
1: 05 # [1]. subjectSignatureAlgorithm=5: unsigned
2: 66 # [2]. subject=char[6]
3: 783235353139 # "x25519"
9: 08 # [3]. subjectPublicKeyAlg=8: X25519
10: 58 20 # [4]. subject public key=EC point=byte[32]
12: 8AFF516FAC71244150E70F9277F4ADF7FB29F41A7A4A8828BD476722FC1B
42: 7F08
44: 82 # [5]. attributes=array[2]
 # attribute[0]
45: 02 # type=2: PrivateKeyPossessionStatement
46: 83 # array[3]
47: 6B # issuer=char[11]
48: 64656D6F20697373756572 # "demo issuer"
59: 41 # certificateSerialNumber=byte[1]
60: 02
61: F6 # cert=<null>
62: 40 # [6]. signature value=byte[0]

```

#### 8.7. Unsigned PoP With X25519 Key And Cert

- \* Signature algorithm: unsigned
- \* CR attributes: a privateKeyPossessionStatement attribute with the cert field.

##### 8.7.1. Private Key

```

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

```

##### 8.7.2. X.509 Certification Request

PEM content (433 bytes):

```

-----BEGIN CERTIFICATE REQUEST-----
MIIBrTCCAzoCAQAwGjEYMBYGA1UEAwPeDI1NTE5LXdpdGhjZXJ0MCowBQYDK2Vu
AyEAiv9Rb6xxJEFQ5w+Sd/St9/sp9Bp6SogovUdnIvwbfiwgggFLMIIBRwYKKwYB
BAGBrGACATGCATcwggEzMCgwIjEgMB4GA1UEAwXc2ltcGxlLXNlbGZzaWduLWVk
MjU1MTkCAhI0MIIBBTcBUKADAgEAgISNDAFBgMrZXAwIjEgMB4GA1UEAwXc2lt
cGxlLXNlbGZzaWduLWVkmjU1MTkwHhcNMjUwMTAyMDAwMDAwWhcNMjUwMTAyMDAw
MDAwWjAiMSAwHgYDVQQDDDBdzaW1wbGUtc2VsZnNpZ24tZWQyNTUxOTAqMAUGAyt1
cAMhAEYnCuwPMoN+Eod50wsknFMdbULBrCnkAjkO3Hn6wr6VoxIwEDA0BgNVHQ8B
Af8EBAMCB4AwBQYDK2VwA0EAwGTwfCZY8TtRPUpq5Vx0jzPeWf6+9hwRP+nXABcW
E8oMcEZNclJc8efHyETF27vSZ0BcAPfdnm5f7YwaytWyCTAKBggrBgEFBQcGJAMB
AA==
-----END CERTIFICATE REQUEST-----

```

Text representation:

Certificate Request:

Data:

Version: v1 (0)

Subject: CN=x25519-withcert

Subject Public Key Info:

Public Key Algorithm: X25519

Pub:

8a:ff:51:6f:ac:71:24:41:50:e7:0f:92:77:f4:ad:f7:fb:29:  
f4:1a:7a:4a:88:28:bd:47:67:22:fc:1b:7f:08

Attributes:

PrivateKeyPossessionStatement:

signer:

Issuer: CN=simple-selfsign-ed25519

Serial Number:

12:34

cert:

Certificate:

Version: v3 (2)

Serial Number:

12:34

Issuer: CN=simple-selfsign-ed25519

Validity:

Not Before: Thu Jan 02 01:00:00 CET 2025

Not After : Fri Jan 02 01:00:00 CET 2026

Subject: CN=simple-selfsign-ed25519

Subject Public Key Info:

Public Key Algorithm: ED25519

Pub:

46:27:0a:ec:0f:32:83:7e:12:87:79:d3:0b:24:9c:53:1d:  
6d:42:c1:ac:29:e4:02:32:8e:dc:79:fa:c2:be:95

X509v3 extensions:

X509v3 keyUsage: critical

digitalSignature

Signature Algorithm: ED25519

Signature Value:

c2:04:f0:7c:26:58:f1:3b:51:3d:4a:a9:e5:5c:74:8f:33:de:  
59:fe:be:f6:1c:11:3f:e9:d7:00:17:16:13:ca:0c:70:46:4d:  
73:52:5c:f1:e7:c7:c8:44:c5:db:bb:d2:67:40:5c:00:f7:dd:  
9e:6e:5f:ed:8c:1a:ca:d5:b2:09

Signature Algorithm: unsigned

Signature Value: <empty>

### 8.7.3. C509 Type 3 Certification Request

- \* C509 type 3 certification request converted from the X.509 certification request in Section 8.7.2.

Plain hex (227 bytes):

```
03056F7832353531392D77697468636572740858208AFF516FAC71244150E70F9277
F4ADF7FB29F41A7A4A8828BD476722FC1B7F088202837773696D706C652D73656C66
7369676E2D656432353531394212348B034212340CF61A6775D7001A69570A807773
696D706C652D73656C667369676E2D656432353531390C582046270AEC0F32837E12
8779D30B249C531D6D42C1AC29E402328EDC79FAC2BE95205840C204F07C2658F13B
513D4AA9E55C748F33DE59FEBEF61C113FE9D700171613CA0C70464D73525CF1E7C7
C844C5DBBBD267405C00F7DD9E6E5FED8C1ACAD5B20940
```

Annotated hex:

- \* See the annotated hex for the C509 type 2 certification request in Section 8.7.4. The only differences are the certification request type and the signature value.

#### 8.7.4. C509 Type 2 Certification Request

Plain hex (227 bytes):

```
02056F7832353531392D77697468636572740858208AFF516FAC71244150E70F9277
F4ADF7FB29F41A7A4A8828BD476722FC1B7F088202837773696D706C652D73656C66
7369676E2D656432353531394212348B024212340CF61A6775D7001A69570A807773
696D706C652D73656C667369676E2D656432353531390C582046270AEC0F32837E12
8779D30B249C531D6D42C1AC29E402328EDC79FAC2BE9520584025623EF44534BC07
269D6071FB3BBBA8F22FF3ED3B65B5C85456151C0F5F9FC259C2932C1F3184D50888
23EBB0B85AE5B7FE9578D2778F10E088944ACB28CC0740
```

Annotated hex:

```

0: 02 # [0]. c509CertificationRequestType=2
1: 05 # [1]. subjectSignatureAlgorithm=5: unsigned
2: 6F # [2]. subject=char[15]
3: 7832353531392D7769746863657274 # "x25519-withcert"
18: 08 # [3]. subjectPublicKeyAlg=8: X25519
19: 58 20 # [4]. subject public key=EC point=byte[32]
21: 8AFF516FAC71244150E70F9277F4ADF7FB29F41A7A4A8828BD476722FC1B
51: 7F08
53: 82 # [5]. attributes=array[2]
 # attribute[0]
54: 02 # type=2: PrivateKeyPossessionStatement
55: 83 # array[3]
56: 77 # issuer=char[23]
57: 73696D706C652D73656C667369676E2D # "simple-selfsign-"
73: 65643235353139 # "ed25519"
80: 42 # certificateSerialNumber=byte[2]
81: 1234
83: 8B # cert=array[11]
84: 02 # [0]. certificate type=2
85: 42 # [1]. certificateSerialNumber=byte[2]
86: 1234
88: 0C # [2]. signature alg=12: Ed25519
89: F6 # [3]. issuer=<null>
90: 1A 6775D700 # [4]. notBefore=1735776000:
 # 2025-01-02T00:00:00Z
95: 1A 69570A80 # [5]. notAfter=1767312000:
 # 2026-01-02T00:00:00Z
100: 77 # [6]. subject=char[23]
101: 73696D706C652D73656C667369676E # "simple-selfsign"
116: 2D65643235353139 # "-ed25519"
124: 0C # [7]. subjectPublicKeyAlg=12: Ed25519
125: 58 20 # [8]. subject public key=EC
 # point=byte[32]
127: 46270AEC0F32837E128779D30B249C531D6D42C1AC29E40232
152: 8EDC79FAC2BE95
159: 20 # [9]. extensions=-1, KeyUsage,
 # critical: [digitalSignature]
160: 58 40 # [10]. signature value=byte[64]
162: 25623EF44534BC07269D6071FB3BBBA8F22FF3ED3B65B5C854
187: 56151C0F5F9FC259C2932C1F3184D5088823EBB0B85AE5B7FE
212: 9578D2778F10E088944ACB28CC07
226: 40 # [6]. signature value=byte[0]

```

## 9. Certification Requests With Different CR Attributes

### 9.1. With Empty CR Attributes

- \* CR attributes: none.

See Section 8.4 and Section 8.5.

### 9.2. With challengePassword Attribute

- \* CR attributes: one challengePassword attribute of type UTF8String.

See Section 8.3.

- \* CR attributes: one challengePassword attribute of type PrintableString.

See Section 8.2.

### 9.3. With extensionRequest Attribute

- \* CR attributes: one extensionRequest attribute.

See Section 8.1.

### 9.4. With privateKeyPossessionStatement Attribute

- \* CR attributes: one privateKeyPossessionStatement attribute without the cert field.

See Section 8.6.

- \* CR attributes: one privateKeyPossessionStatement attribute with the cert field.

See Section 8.7.

## 10. Certification Request Templates

### 10.1. All Fields Set to "undefined" Where Possible

- \* c509CertificationRequestType: undefined
- \* subjectSignatureAlgorithm: undefined
- \* subject: undefined
- \* subjectPublicKeyAlgorithm: undefined

```
* subjectPublicKey: undefined
* extensionsRequest: undefined
```

Plain hex (7 bytes):

00F7F7F7F7F7F7

Annotated hex:

|       |                                                 |
|-------|-------------------------------------------------|
| 0: 00 | # [0]. c509CertificationRequestTemplateType=0   |
| 1: F7 | # [1]. c509CertificationRequestType=<undefined> |
| 2: F7 | # [2]. subjectSignatureAlgorithm=<undefined>    |
| 3: F7 | # [3]. subject=<undefined>                      |
| 4: F7 | # [4]. subjectPublicKeyAlgorithm=<undefined>    |
| 5: F7 | # [5]. subjectPublicKey=<undefined>             |
| 6: F7 | # [6]. extensions=<undefined>                   |

#### 10.2. With One Element in Each Field

```
* c509CertificationRequestType: one element
* subjectSignatureAlgorithm: one element
* subject: one element
* subjectPublicKeyAlgorithm: one element
* extensionsRequest: one element
```

Plain hex (17 bytes):

008102810084010101F78101F78303F4F7

Annotated hex:

```

0: 00 # [0]. c509CertificationRequestTemplateType=0
1: 81 # [1]. c509CertificationRequestType=array[1]
2: 02 # 2
3: 81 # [2]. subjectSignatureAlgorithm=array[1]
4: 00 # [0]=0: ecdsa-with-sha256
5: 84 # [3]. subject=array[4], 1 attribute
 # attribute[0]
6: 01 # type=1: commonName
7: 01 # minOccurs=1
8: 01 # maxOccurs=1
9: F7 # value=<undefined>
10: 81 # [4]. subjectPublicKeyAlgorithm=array[1]
11: 01 # [0]=1: EC public key on curve secp256r1
12: F7 # [5]. subjectPublicKey=<undefined>
13: 83 # [6]. extensions=array[3]
 # extension[0]
14: 03 # type=3: SubjectAlternativeName
15: F4 # required
16: F7 # value=<undefined>

```

### 10.3. Complex Template

```

* c509CertificationRequestType: multiple values

* 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 (152 bytes):

```
008202038301492B0601040181FD590982492B0601040181FD590A42050090010101
F7040101624445492B0601040181FD590B0101F7492B0601040181FD590C01014D0C
0B636F6E73742D76616C75658301492B0601040181FD590982492B0601040181FD59
0A420500F78C08F4F702F51860492B0601040181FD590DF4F7492B0601040181FD59
0EF44D0C0B636F6E73742D76616C7565
```

Annotated hex:

```
0: 00 # [0]. c509CertificationRequestTemplateType=0
1: 82 # [1]. c509CertificationRequestType=array[2]
2: 02 # 2
3: 03 # 3
4: 83 # [2]. subjectSignatureAlgorithm=array[3]
5: 01 # [0]=1: ecdsa-with-sha384
6: 49 # [1]=byte[9]:
7: 2B0601040181FD5909 # oid: 1.3.6.1.4.1.32473.9
16: 82 # [2]=array[2]
17: 49 # algorithm=byte[9]:
18: 2B0601040181FD590A # oid: 1.3.6.1.4.1.32473.10
27: 42 # parameters=byte[2]
28: 0500
30: 90 # [3]. subject=array[16], 4 attributes
 # attribute[0]
31: 01 # type=1: commonName
32: 01 # minOccurs=1
33: 01 # maxOccurs=1
34: F7 # value=<undefined>
 # attribute[1]
35: 04 # type=4: country
36: 01 # minOccurs=1
37: 01 # maxOccurs=1
38: 62 # value=char[2]
39: 4445 # "DE"
 # attribute[2]
41: 49 # type=byte[9]:
42: 2B0601040181FD590B # oid: 1.3.6.1.4.1.32473.11
51: 01 # minOccurs=1
52: 01 # maxOccurs=1
53: F7 # value=<undefined>
 # attribute[3]
54: 49 # type=byte[9]:
55: 2B0601040181FD590C # oid: 1.3.6.1.4.1.32473.12
64: 01 # minOccurs=1
65: 01 # maxOccurs=1
66: 4D # value=byte[13]
67: 0C0B636F6E73742D76616C7565
```

```

80: 83 # [4]. subjectPublicKeyAlgorithm=array[3]
81: 01 # [0]=1: EC public key on curve secp256r1
82: 49 # [1]=byte[9]:
83: 2B0601040181FD5909 # oid: 1.3.6.1.4.1.32473.9
92: 82 # [2]=array[2]
93: 49 # algorithm=byte[9]:
94: 2B0601040181FD590A # oid: 1.3.6.1.4.1.32473.10
103: 42 # parameters=byte[2]
104: 0500
106: F7 # [5]. subjectPublicKey=<undefined>
107: 8C # [6]. extensions=array[12]
 # extension[0]
108: 08 # type=8: ExtendedKeyUsage
109: F4 # required
110: F7 # value=<undefined>
 # extension[1]
111: 02 # type=2: KeyUsage
112: F5 # optional
113: 18 60 # value=96: [keyCertSign, cRLSign]
 # extension[2]
115: 49 # type=byte[9]:
116: 2B0601040181FD590D # oid: 1.3.6.1.4.1.32473.13
125: F4 # required
126: F7 # value=<undefined>
 # extension[3]
127: 49 # type=byte[9]:
128: 2B0601040181FD590E # oid: 1.3.6.1.4.1.32473.14
137: F4 # required
138: 4D # value=byte[13]
139: 0C0B636F6E73742D76616C7565

```

## 11. Security Considerations

The private keys shown in this document are for example purposes only. They are not secret and MUST NOT be used in deployments.

The examples use 1024-bit or 1536-bit RSA keys and reuse key pairs to keep the examples compact. In deployments, key pairs are expected to be generated uniquely and not reused. The examples also use RSA PKCS#1 v1.5 signatures and SHA-1 to cover all signature algorithms defined in [I-D.ietf-cose-cbor-encoded-cert]. These choices do not reflect current state-of-the-art security recommendations; at the time of writing, RSA keys of at least 3072 bits, stronger hash functions, and RSA-PSS are required for adequate security.

## 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., Furuheid, M., and L. Liao, "CBOR Encoded X.509 Certificates (C509 Certificates)", Work in Progress, Internet-Draft, draft-ietf-cose-cbor-encoded-cert-19, 11 May 2026, <<https://datatracker.ietf.org/doc/html/draft-ietf-cose-cbor-encoded-cert-19>>.
- [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/>>.

Acknowledgments

Authors' Addresses

Lijun Liao  
NIO  
Email: [lijun.liao@nio.io](mailto:lijun.liao@nio.io)

Gran Selander  
Ericsson  
Email: [goran.selander@ericsson.com](mailto:goran.selander@ericsson.com)

John Preu Mattsson  
Ericsson  
Email: [john.mattsson@ericsson.com](mailto:john.mattsson@ericsson.com)