CBOR Encoded X.509 Certificates (C509 Certificates)

Abstract

This document specifies a CBOR encoding of X.509 certificates. The resulting certificates are called C509 Certificates. The CBOR encoding supports a large subset of RFC 5280 and all certificates compatible with the RFC 7925, IEEE 802.1AR (DevID), CNSA, RPKI, GSMA eUICC, and CA/Browser Forum Baseline Requirements profiles. When used to re-encode DER encoded X.509 certificates, the CBOR encoding can in many cases reduce the size of RFC 7925 profiled certificates with over 50%. The CBOR encoded structure can alternatively be signed directly ("natively signed"), which does not require re-encoding for the signature to be verified. The document also specifies C509 COSE headers, a C509 TLS certificate type, and a C509 file format.

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 11 January 2023.

Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the document authors. All rights reserved.
1. Introduction
2. Notational Conventions
3. C509 Certificate
   3.1. Message Fields
   3.2. Encoding of subjectPublicKey and issuerSignatureValue
   3.3. Encoding of Extensions
4. C509 Certificate Signing Request
5. C509 Certificate Revocation List
7. C509 Processing and Certificate Issuance
8. Legacy Considerations
9. Expected Certificate Sizes
10. Security Considerations
11. IANA Considerations
    11.1. C509 Certificate Types Registry
    11.2. C509 Attributes Registry
    11.3. C509 Extensions Registry
    11.4. C509 Certificate Policies Registry
    11.5. C509 Policies Qualifiers Registry
    11.6. C509 Information Access Registry
    11.7. C509 Extended Key Usages Registry
    11.8. C509 General Names Registry
    11.9. C509 Signature Algorithms Registry
    11.10. C509 Public Key Algorithms Registry
    11.11. COSE Header Parameters Registry
    11.12. TLS Certificate Types Registry
    11.13. CBOR Tags Registry
12. References
    12.1. Normative References
    12.2. Informative References
Appendix A. Example C509 Certificates
   A.1. Example RFC 7925 profiled X.509 Certificate
   A.2. Example IEEE 802.1AR profiled X.509 Certificate
   A.3. Example CAB Baseline ECDSA HTTPS X.509 Certificate
   A.4. Example CAB Baseline RSA HTTPS X.509 Certificate
Acknowledgments
Authors' Addresses
1. Introduction

One of the challenges with deploying a Public Key Infrastructure (PKI) for the Internet of Things (IoT) is the size and parsing of X.509 public key certificates [RFC5280], since those are not optimized for constrained environments [RFC7228]. Large certificate chains are also problematic in non-constrained protocols such as EAP-TLS [RFC9190] [RFC9191] where authenticators typically drop an EAP session after only 40 - 50 round-trips, QUIC [RFC9000] where the latency increases significantly unless the server sends less than three times as many bytes as received prior to validating the client address, and RPKI [RFC6487] where a single certificate can be very large. More compact certificate representations are therefore desirable in many use cases. Due to the current PKI usage of DER encoded X.509 certificates, keeping compatibility with DER encoded X.509 is necessary at least for a transition period. However, the use of a more compact encoding with the Concise Binary Object Representation (CBOR) [RFC8949] reduces the certificate size significantly which has known performance benefits in terms of decreased communication overhead, power consumption, latency, storage, etc.

CBOR is a data format designed for small code size and small message size. CBOR builds on the JSON data model but extends it by e.g. encoding binary data directly without base64 conversion. In addition to the binary CBOR encoding, CBOR also has a diagnostic notation that is readable and editable by humans. The Concise Data Definition Language (CDDL) [RFC8610] provides a way to express structures for protocol messages and APIs that use CBOR. RFC 8610 also extends the diagnostic notation.

CBOR data items are encoded to or decoded from byte strings using a type-length-value encoding scheme, where the three highest order bits of the initial byte contain information about the major type. CBOR supports several different types of data items, in addition to integers (int, uint), simple values (e.g. null), byte strings (bstr), and text strings (tstr), CBOR also supports arrays [] of data items, maps {} of pairs of data items, and sequences of data items. For a complete specification and examples, see [RFC8949], [RFC8610], and [RFC8742]. We recommend implementors to get used to CBOR by using the CBOR playground [Cborme].

CAB Baseline Requirements [CAB-TLS], RFC 7925 [RFC7925], IEEE 802.1AR [IEEE-802.1AR], and CNSA [RFC8603] specify certificate profiles which can be applied to certificate based authentication with, e.g., TLS [RFC8446], QUIC [RFC9000], DTLS [RFC9147], COSE [RFC8152], EDHOC [I-D.ietf-lake-edhoc], or Compact TLS 1.3 [I-D.ietf-tls-cts]. RFC 7925 [RFC7925], RFC7925bis [I-D.ietf-uta-tls13-iot-profile], and IEEE 802.1AR [IEEE-802.1AR] specifically
target Internet of Things deployments. This document specifies a CBOR encoding based on [X.509-IoT], which can support large parts of RFC 5280. The encoding supports all RFC 7925, IEEE 802.1AR, CAB Baseline [CAB-TLS], [CAB-Code], RPKI [RFC6487], eUICC [GSMA-eUICC] profiled X.509 certificates. The resulting certificates are called C509 Certificates. This document does not specify a certificate profile. Two variants are defined using the same CBOR encoding and differing only in what is being signed:

1. An invertible CBOR re-encoding of DER encoded X.509 certificates [RFC5280], which can be reversed to obtain the original DER encoded X.509 certificate.

2. Natively signed C509 certificates, where the signature is calculated over the CBOR encoding instead of over the DER encoding as in 1. This removes the need for ASN.1 and DER parsing and the associated complexity but they are not backwards compatible with implementations requiring DER encoded X.509.

Natively signed C509 certificates can be applied in devices that are only required to authenticate to natively signed C509 certificate compatible servers, which is not a major restriction for many IoT deployments where the parties issuing and verifying certificates can be a restricted ecosystem.

This document specifies COSE headers for use of the C509 certificates with COSE, see Section 11.11. The document also specifies a TLS certificate type for use of the C509 certificates with TLS and QUIC (with or without additional TLS certificate compression), see Section 11.12.

2. Notational Conventions

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.

This specification makes use of the terminology in [RFC5280], [RFC7228], [RFC8610], and [RFC8949]. When referring to CBOR, this specification always refers to Deterministically Encoded CBOR as specified in Sections 4.2.1 and 4.2.2 of [RFC8949].

3. C509 Certificate

This section specifies the content and encoding for C509 certificates, with the overall objective to produce a very compact representation supporting large parts of [RFC5280], and everything
in [RFC7925], [IEEE-802.1AR], RPKI [RFC6487], GSMA eUICC [GSMA-eUICC], and CAB Baseline [CAB-TLS] [CAB-Code]. In the CBOR encoding, static fields are elided, elliptic curve points and time values are compressed, OID are replaced with short integers, and redundant encoding is removed. Combining these different components reduces the certificate size significantly, which is not possible with general purpose compression algorithms, see Figure 5.

The C509 certificate can be either a CBOR re-encoding of a DER encoded X.509 certificate, in which case the signature is calculated on the DER encoded ASN.1 data in the X.509 certificate, or a natively signed C509 certificate, in which case the signature is calculated directly on the CBOR encoded data. In both cases the certificate content is adhering to the restrictions given by [RFC5280]. The re-encoding is known to work with DER encoded certificates but might work with other canonical encodings. The re-encoding does not work for BER encoded certificates.

In the encoding described below, the order of elements in arrays are always encoded in the same order as the elements or the corresponding SEQUENCE or SET in the DER encoding.

3.1. Message Fields

The X.509 fields and their CBOR encodings are listed below, and used in the definition of C509 certificates, see Figure 1.

C509 certificates are defined in terms of DER encoded [RFC5280] X.509 certificates:

*version. The 'version' field is encoded in the 'c509CertificateType' CBOR int. The field 'c509CertificateType' also indicates the type of the C509 certificate. Currently, the type can be a natively signed C509 certificate following X.509 v3 (c509CertificateType = 0) or a CBOR re-encoded X.509 v3 DER certificate (c509CertificateType = 1), see Section 11.1.

*serialNumber. The 'serialNumber' INTEGER value field is encoded as the unwrapped CBOR unsigned bignum (~biguint) 'certificateSerialNumber'. Any leading 0x00 byte (to indicate that the number is not negative) is therefore omitted.

*signature. The 'signature' field is always the same as the 'signatureAlgorithm' field and therefore omitted from the CBOR encoding.

*issuer. In the general case, the sequence of 'RelativeDistinguishedName' is encoded as a CBOR array of CBOR arrays of Attributes. Typically, each RelativeDistinguishedName only contains a single attribute and the sequence is then encoded
as a CBOR array of Attributes. Each Attribute is encoded as a (CBOR int, CBOR text string) pair or as a (unwrapped CBOR OID, CBOR bytes) pair. The absolute value of the CBOR int (see Figure 7) encodes the attribute type and the sign is used to represent the character string type; positive for Utf8String, negative for PrintableString. The Attribute Email Address is always an IA5String. In natively signed C509 certificates all text strings are UTF-8 encoded and all attributeType SHALL have be non-negative. Text strings SHALL still adhere to any X.509 restrictions, i.e., serialNumber SHALL only contain the 74 character subset of ASCII allowed by PrintableString and countryName SHALL have length 2. The string types teletexString, universalString, and bmpString are not supported. If Name contains a single Attribute containing an utf8String encoded 'common name' it is encoded as a CBOR text string. If the text string contains an EUI-64 of the form "HH-HH-HH-HH-HH-HH-HH-HH" where 'H' is one of the symbols '0'-'9' or 'A'-'F' it is encoded as a CBOR byte string of length 8 instead. EUI-64 mapped from a 48-bit MAC address (i.e., of the form "HH-HH-HH-FF-FE-HH-HH-HH") is encoded as a CBOR byte string of length 6.

*validity. The 'notBefore' and 'notAfter' fields are encoded as unwrapped CBOR epoch-based date/time (~time) where the tag content is an unsigned integer. In POSIX time, leap seconds are ignored, with a leap second having the same POSIX time as the second before it. Compression of X.509 certificates with the time 23:59:60 UTC is therefore not supported. Note that RFC 5280 mandates encoding of dates through the year 2049 as UTCTime, and later dates as GeneralizedTime. The value "99991231235959Z" (no expiration date) is encoded as CBOR null.

*subject. The 'subject' is encoded exactly like issuer.

*subjectPublicKeyInfo. The 'AlgorithmIdentifier' field including parameters is encoded as the CBOR int 'subjectPublicKeyAlgorithm' (see Section 11.10) or as an array with an unwrapped CBOR OID tag [RFC9090] optionally followed by the parameters encoded as a CBOR byte string. In general, the 'subjectPublicKey' BIT STRING value field is encoded as a CBOR byte string. This specification assumes the BIT STRING has zero unused bits and the unused bits byte is omitted. For rsaEncryption and id-ecPublicKey, the encoding of subjectPublicKey is further optimized as described in Section 3.2.

*issuerUniqueID. Not supported.

*subjectUniqueID. Not supported.
extensions. The 'extensions' field is encoded as a CBOR array
where each extension is encoded as either a CBOR int (see Section
11.3) followed by an optional CBOR item of any type or an
unwrapped CBOR OID tag [RFC9090] followed by a CBOR bool encoding
'critical' and the DER encoded value of the 'extnValue' encoded
as a CBOR byte string. If the array contains exactly two ints and
the absolute value of the first int is 2 (corresponding to
keyUsage), the array is omitted and the extensions is encoded as
a single CBOR int with the absolute value of the second int and
the sign of the first int. Extensions are encoded as specified in
Section 3.3. The extensions mandated to be supported by [RFC7925]
and [IEEE-802.1AR] are given special treatment. An omitted
'extensions' field is encoded as an empty CBOR array.

*signatureAlgorithm. The 'signatureAlgorithm' field including
parameters is encoded as a CBOR int (see Section 11.9) or as an
array with an unwrapped CBOR OID tag [RFC9090] optionally
followed by the parameters encoded as a CBOR byte string.

*signatureValue. In general, the 'signatureValue' BIT STRING value
field is encoded as the CBOR byte string issuerSignatureValue.
This specification assumes the BIT STRING has zero unused bits
and the unused bits byte is omitted. For natively signed C509
certificates the signatureValue is calculated over the CBOR
sequence TBSCertificate. For ECDSA, the encoding of
issuerSignatureValue is further optimized as described in Section
3.2

The following Concise Data Definition Language (CDDL) defines the
CBOR array C509Certificate and the CBOR sequence [RFC8742]
TBSCertificate. The member names therefore only have documentary
value. Applications not requiring a CBOR item MAY represent C509
certificates with the CBOR sequence ~C509Certificate (unwrapped
C509Certificate).
C509Certificate = [  
  TBSCertificate,  
  issuerSignatureValue : any,  
]

; The elements of the following group are used in a CBOR Sequence:
TBSCertificate = (  
  c509CertificateType: int,  
  certificateSerialNumber: CertificateSerialNumber,  
  issuer: Name,  
  validityNotBefore: Time,  
  validityNotAfter: Time,  
  subject: Name,  
  subjectPublicKeyAlgorithm: AlgorithmIdentifier,  
  subjectPublicKey: any,  
  extensions: Extensions,  
  issuerSignatureAlgorithm: AlgorithmIdentifier,  
)

CertificateSerialNumber = ~biguint

Name = [ * RelativeDistinguishedName ] / text / bytes

RelativeDistinguishedName = Attribute / [ 2* Attribute ]

Attribute = ( attributeType: int, attributeValue: text ) //  
          ( attributeType: ~oid, attributeValue: bytes )

Time = ~time / null

AlgorithmIdentifier = int / ~oid /  
                     [ algorithm: ~oid, parameters: bytes ]

Extensions = [ * Extension ] / int

Extension = ( extensionID: int, extensionValue: any ) //  
            ( extensionID: ~oid, ? critical: true,  
              extensionValue: bytes )

Figure 1: CDDL for C509Certificate.

3.2. Encoding of subjectPublicKey and issuerSignatureValue

3.2.1. Encoding of subjectPublicKey

For RSA public keys (rsaEncryption), the SEQUENCE and INTEGER type and length fields are omitted and the two INTEGER value fields (modulus, exponent) are encoded as an array of two unwrapped CBOR unsigned bignum (~biguint), i.e. [ modulus : ~biguint, exponent : ~biguint ]. If the exponent is 65537, the array and the exponent is
omitted and subjectPublicKey consist of only the modulus encoded as an unwrapped CBOR unsigned bignum (~biguint).

For elliptic curve public keys in Weierstrass form (id-ecPublicKey), uncompressed keys are point compressed as defined in Section 2.3.3 of [SECG]. If a DER encoded certificate with a point compressed public key of type id-ecPublicKey is CBOR encoded, the octets 0xfe and 0xfd are used instead of 0x02 and 0x03 in the CBOR encoding to represent even and odd y-coordinate, respectively.

3.2.2. Encoding of issuerSignatureValue

For ECDSA signatures, the SEQUENCE and INTEGER type and length fields as well as the any leading 0x00 byte (to indicate that the number is not negative) are omitted. If the two INTEGER value fields have different lengths, the shortest INTEGER value field is padded with zeroes so that the two fields have the same length. The resulting byte string is encoded as a CBOR byte string.

3.3. Encoding of Extensions

This section details the encoding of the 'extensions' field. The 'extensions' field is encoded as a CBOR array where each extensionID is encoded as either a CBOR int or an unwrapped CBOR OID tag. If 'extensionID' is encoded an int (see Section 11.3), the sign is used to encode if the extension is critical and the 'critical' field is omitted. Critical extensions are encoded with a negative sign and non-critical extensions are encoded with a positive sign.

The 'extnValue' OCTET STRING value field is encoded as the CBOR byte string 'extensionValue' except for the extensions specified below. For some extensions, only commonly used parts are supported by the CBOR encoding. If unsupported parts are used, the CBOR encoding cannot be used.

CBOR encoding of the following extension values are fully supported:

*Subject Key Identifier (subjectKeyIdentifier). The extensionValue is encoded as follows:

KeyIdentifier = bytes
SubjectKeyIdentifier = KeyIdentifier

*Key Usage (keyUsage). The 'KeyUsage' BIT STRING is interpreted as an unsigned integer in network byte order and encoded as a CBOR int. See Section 3.1 for special encoding in case keyUsage is the only extension present.
Policy Mappings (policyMappings). extensionValue is encoded as follows:

PolicyMappings = [ + (issuerDomainPolicy: ~oid, subjectDomainPolicy: ~oid) ]

*Basic Constraints (basicConstraints). If 'cA' = false then extensionValue = -2, if 'cA' = true and 'pathLenConstraint' is not present then extensionValue = -1, and if 'cA' = true and 'pathLenConstraint' is present then extensionValue = pathLenConstraint.

BasicConstraints = int

*Policy Constraints (policyConstraints). extensionValue is encoded as follows:


*Extended Key Usage (extKeyUsage). extensionValue is encoded as an array of CBOR ints (see Section 11.7 or unwrapped CBOR OID tags [RFC9090] where each int or OID tag encodes a key usage purpose. If the array contains a single KeyPurposeId, the array is omitted.

KeyPurposeId = int / ~oid
ExtKeyUsageSyntax = [ 2* KeyPurposeId ] / KeyPurposeId

*Inhibit anyPolicy (inhibitAnyPolicy). extensionValue is encoded as follows:

InhibitAnyPolicy = uint

CBOR encoding of the following extension values are partly supported:

*Subject Alternative Name (subjectAltName). If the subject alternative name only contains general names registered in Section 11.8 the extension value can be CBOR encoded. extensionValue is encoded as an array of (int, any) pairs where each pair encodes a general name (see Section 11.8). If subjectAltName contains exactly one dNSName, the array and the int are omitted and extensionValue is the dNSName encoded as a CBOR text string. In addition to the general names defined in
[RFC5280], the hardwareModuleName type of otherName has been
given its own int due to its mandatory use in IEEE 802.1AR. When
'otherName + hardwareModuleName' is used, then [ oid, bytes ] is
used to identify the pair ( hwType, hwSerialEntries ) directly as
specified in [RFC4108]. Only the general names in Section 11.8
are supported.

GeneralName = ( GeneralNameType : int, GeneralNameValue : any )
GeneralNames = [ + GeneralName ]
SubjectAltName = GeneralNames / text

*Issuer Alternative Name (issuerAltName). extensionValue is
encoded exactly like subjectAltName.

IssuerAltName = GeneralNames / text

*CRL Distribution Points (cRLDistributionPoints). If the CRL
Distribution Points is a sequence of DistributionPointName, where
each DistributionPointName only contains
uniformResourceIdentifiers, the extension value can be CBOR
coded. extensionValue is encoded as follows:

DistributionPointName = [ 2* text ] / text
CRLDistributionPoints = [ + DistributionPointName ]

*Freshest CRL (freshestCRL). extensionValue is encoded exactly
like cRLDistributionPoints.

FreshestCRL = CRLDistributionPoints

*Authority Information Access (authorityInfoAccess). If all the
GeneralNames in authorityInfoAccess are of type
uniformResourceIdentifier, the extension value can be CBOR
encoded. Each accessMethod is encoded as an CBOR ints (see
Section 11.6) or unwrapped CBOR OID tags [RFC9090]. The
uniformResourceIdentifiers are encoded as CBOR text strings.

AccessDescription = ( accessMethod: int / ~oid , uri: text )
AuthorityInfoAccessSyntax = [ + AccessDescription ]

*Subject Information Access (subjectInfoAccess). Encoded exactly
like authorityInfoAccess.

SubjectInfoAccessSyntax = AuthorityInfoAccessSyntax

*Authority Key Identifier (authorityKeyIdentifier). If the
authority key identifier contains all of keyIdentifier,
certIssuer, and certSerialNumberm or if only keyIdentifier is
present the extension value can be CBOR encoded. If all three are
present a CBOR array is used, if only keyIdentifier is present, the array is omitted:

KeyIdentifierArray = [
  keyIdentifier: KeyIdentifier,
  authorityCertIssuer: GeneralNames,
  authorityCertSerialNumber: CertificateSerialNumber
]
AuthorityKeyIdentifier = KeyIdentifierArray / KeyIdentifier

*Certificate Policies (certificatePolicies). If noticeRef is not used and any explicitText are encoded as UTF8String, the extension value can be CBOR encoded. OIDs registered in Section 11.4 are encoded as an int. The policyQualifierId is encoded as an CBOR int (see Section 11.5) or an unwrapped CBOR OID tag [RFC9090].

PolicyIdentifier = int / ~oid
PolicyQualifierInfo = (policyQualifierId: int / ~oid, qualifier: text,
) CertificatePolicies = [
  + (PolicyIdentifier, ? [ + PolicyQualifierInfo ] )
]

*Name Constraints (nameConstraints). If the name constraints only contains general names registered in Section 11.8 the extension value can be CBOR encoded.

GeneralSubtree = [ GeneralName, minimum: uint, ? maximum: uint ]
NameConstraints = [permittedSubtrees: GeneralSubtree,
  excludedSubtrees: GeneralSubtree,
]

*Subject Directory Attributes (subjectDirectoryAttributes). Encoded as attributes in issuer and subject with the difference that there can be more than one attributeValue.

Attributes = ( attributeType: int, attributeValue: [+text] ) //
  ( attributeType: ~oid, attributeValue: [+bytes] )
SubjectDirectoryAttributes = Attributes

*AS Resources (autonomousSysIds). If rdi is not present, the extension value can be CBOR encoded. Each ASId is encoded as an uint. With the exception of the first ASId, the ASid is encoded as the difference to the previous ASId.
AsIdsOrRanges = uint / [uint, uint]
ASIdentifiers = [ + AsIdsOrRanges ] / null

*AS Resources v2 (id-pe-ipAddrBlocks-v2). Encoded exactly like autonomousSysIds.

*IP Resources (id-pe-ipAddrBlocks). If rdi and SAFI is not present, the extension value can be CBOR encoded. Each AddressPrefix is encoded as a CBOR bytes string (without the unused bits octet) followed by the number of unused bits encoded as a CBOR uint. Each AddressRange is encoded as an array of two CBOR byte strings. The unused bits for min and max are omitted, but the unused bits in max IPAddress is set to ones. With the exception of the first Address, if the byte string has the same length as the previous ASid, the Addrress is encoded as an uint with the the difference to the previous Address.

Address = bytes / uint,
AddressPrefix = (Address, unusedBits: uint)
AddressRange = [Address, Address]
IPAddressOrRange = AddressPrefix / AddressRange
IPAddressChoice = [ + IPAddressOrRange ] / null
IPAddrBlocks = [ AFI: uint, IPAddressChoice ]

*IP Resources v2 (id-pe-ipAddrBlocks-v2). Encoded exactly like id-pe-ipAddrBlocks.

*Signed Certificate Timestamp. If all the SCTs are version 1, and there are no SCT extensions, the extension value can be CBOR encoded. LogIDs are encoded as CBOR byte strings, the timestamp is encoded as and CBOR int (milliseconds since validityNotBefore), and the signature is encoded with an (AlgorithmIdentifier, any) pair in the same way as issuerSignatureAlgorithm and issuerSignatureValue.

SignedCertificateTimestamp = (logID: bytes,
timestamp: int,
sigAlg: AlgorithmIdentifier,
sigValue: any,
)
SignedCertificateTimestamps = [ + SignedCertificateTimestamp ]

3.3.1. Example Encoding of Extensions

The examples below use values from Section 11.3, Section 11.7, and Section 11.8:

*A critical basicConstraints ('cA' = true) without pathLenConstraint is encoded as the two CBOR ints -4, -1.
*A non-critical keyUsage with digitalSignature and keyAgreement asserted is encoded as the two CBOR ints 2, 17 \((2^0 + 2^4 = 17)\).

*A non-critical extKeyUsage containing id-kp-codeSigning and id-kp-OCSPSigning is encoded as the CBOR int 8 followed by the CBOR array \([ 3, 6 ]\).

*A non-critical subjectAltName containing only the dNSName example.com is encoded as the CBOR int 3 followed by the CBOR text string "example.com".

Thus, the extension field of a certificate containing all of the above extensions in the given order would be encoded as the CBOR array \([-4, -1, 2, 17, 8, [ 3, 6 ], 3, "example.com" ]\).

4. **C509 Certificate Signing Request**

The section defines the C509 Certificate Signing Request (CSR) format based on and compatible with RFC 2986 [RFC2986] reusing the formatting for C509 certificates defined in Section 3. There are currently two c509CertificateSigningRequestType values defined, c509CertificateSigningRequestType = 0 requests a c509CertificateType = 0 and c509CertificateSigningRequestType = 1 requests a c509CertificateType = 1. subjectProofOfPossessionAlgorithm can be a C509 signature algorithm or a non-signature Proof-of-Possession Algorithm as defined in e.g. RFC 6955. CSR attributes other than extensionRequest are not supported.

C509CertificateSigningRequest = [TBSCertificateSigningRequest, subjectProofOfPossessionValue: any,]

; The elements of the following group are used in a CBOR Sequence:TBSCertificateSigningRequest = (c509CertificateSigningRequestType: int, subject: Name, subjectPublicKeyAlgorithm: AlgorithmIdentifier, subjectPublicKey: any, extensionsRequest : Extensions, subjectProofOfPossessionAlgorithm: AlgorithmIdentifier,)

Figure 2: CDDL for C509CertificateSigningRequest.

After verifying the subjectProofOfPossessionValue, the CA MAY transform the C509CertificateSigningRequest into a RFC 2985 CertificationRequestInfo for compatibility with existing procedures and code.
5. C509 Certificate Revocation List

The section defines the C509 Certificate Revocation List (CRL) format based on and compatible with [RFC5280] reusing the formatting for C509 certificates defined in Section 3.

C509CertificateRevocationList = [
   TBSCertificateRevocationList,
   issuerSignatureValue : any,
]

; The elements of the following group are used in a CBOR Sequence:
TBSCertificateSigningRequest = ( 
   C509CertificateRevocationListType: int,
   issuer: Name,
   thisUpdate: Time,
   nextUpdate: Time,
   revokedCertificates: RevokedCertificates,
   crlExtensions: Extensions,
   issuerSignatureAlgorithm: AlgorithmIdentifier,
)

RevokedCertificates = [
   userCertificate: CertificateSerialNumber,
   revocationDate: Time,
   crlEntryExtensions: Extensions,
]

Figure 3: CDDL for C509CertificateRevocationList.


TODO

7. C509 Processing and Certificate Issuance

It is straightforward to integrate the C509 format into legacy X.509 processing during certificate issuance. C509 processing can be performed as an isolated function of the CA, or as a separate function trusted by the CA.

The CSR format defined in Section 4 follows the PKCS#10 format to enable a direct mapping to the certification request information, see Section 4.1 of [RFC2986].

When a certificate request is received the CA, or function trusted by the CA, needs to perform some limited C509 processing and verify the proof of possession of the public key, before normal certificate generation can take place.
In the reverse direction, in case c509CertificateType = 1 was requested, a separate C509 processing function can perform the conversion from a generated X.509 certificate to C509 as a bump-in-the-wire. In case c509CertificateType = 0 was requested, the C509 processing needs to be performed before signing the certificate, in which case a tighter integration with CA may be needed.

8. Legacy Considerations

C509 certificates can be deployed with legacy X.509 certificates and CA infrastructure. In order to verify the signature, the C509 certificate is used to recreate the original X.509 data structure to be able to verify the signature.

For protocols like TLS/DTLS 1.2, where the handshake is sent unencrypted, the actual encoding and compression can be done at different locations depending on the deployment setting. For example, the mapping between C509 certificate and standard X.509 certificate can take place in a 6LoWPAN border gateway which allows the server side to stay unmodified. This case gives the advantage of the low overhead of a C509 certificate over a constrained wireless links. The conversion to X.509 within an IoT device will incur a computational overhead, however, measured in energy this is likely to be negligible compared to the reduced communication overhead.

For the setting with constrained server and server-only authentication, the server only needs to be provisioned with the C509 certificate and does not perform the conversion to X.509. This option is viable when client authentication can be asserted by other means.

For protocols like IKEv2, TLS/DTLS 1.3, and EDHOC, where certificates are encrypted, the proposed encoding needs to be done fully end-to-end, through adding the encoding/decoding functionality to the server.

9. Expected Certificate Sizes

The CBOR encoding of the sample certificate chains given in Appendix A results in the numbers shown in Figure 4 and Figure 5. COSE_X509 is defined in [I-D.ietf-cose-x509] and COSE_C509 is defined in Section 11.11. After RFC 7925 profiling, most duplicated information has been removed, and the remaining text strings are minimal in size. Therefore, the further size reduction reached with general compression mechanisms such as Brotil will be small, mainly corresponding to making the ASN.1 encoding more compact. CBOR encoding can however significantly compress RFC 7925 profiled certificates. For the example HTTPS certificate chains (www.ietf.org and tools.ietf.org) both C509 and Brotil perform well complementing
each other. C509 use dedicated information to compress individual certificates, while Broctli can compress duplicate information in the entire chain. Note that C509 certificates of type 0 and 1 have the same size. For Broctli [RFC7932], the Rust crate Broctli 3.3.0 was used with compression level 11 and window size 22.

Figure 4: Comparing Sizes of Certificate Chains in COSE. Number of bytes (length of certificate chain).

Figure 5: Comparing Sizes of Certificate Chains with TLS. Number of bytes (length of certificate chain). X509 and C509 are Certificate messages. X509 + Broctli and C509 + Broctli are CompressedCertificate messages.

10. Security Considerations

The CBOR profiling of X.509 certificates does not change the security assumptions needed when deploying standard X.509 certificates but decreases the number of fields transmitted, which reduces the risk for implementation errors.

The use of natively signed C509 certificates removes the need for ASN.1 encoding, which is a rich source of security vulnerabilities.
Conversion between the certificate formats can be made in constant time to reduce risk of information leakage through side channels.

The mechanism in this draft does not reveal any additional information compared to X.509. Because of difference in size, it will be possible to detect that this profile is used. The gateway solution described in Section 8 requires unencrypted certificates and is not recommended.

11. IANA Considerations

This document creates several new registries under the new heading "C509 Certificate". For all items, the 'Reference' field points to this document.

The expert reviewers for the registries defined in this document are expected to ensure that the usage solves a valid use case that could not be solved better in a different way, that it is not going to duplicate one that is already registered, and that the registered point is likely to be used in deployments. They are furthermore expected to check the clarity of purpose and use of the requested code points. Experts should take into account the expected usage of entries when approving point assignment, and the length of the encoded value should be weighed against the number of code points left that encode to that size and how constrained the systems it will be used on are. Values in the interval [-24, 23] have a 1 byte encodings, other values in the interval [-256, 255] have a 2 byte encodings, and the remaining values in the interval [-65536, 65535] have 3 byte encodings.

11.1. C509 Certificate Types Registry

IANA has created a new registry titled "C509 Certificate Types" under the new heading "C509 Certificate". The columns of the registry are Value, Description, and Reference, where Value is an integer, and the other columns are text strings. For values in the interval [-24, 23] the registration procedure is "IETF Review" and "Expert Review". For all other values the registration procedure is "Expert Review". For all other values the registration procedure is "Expert Review". The initial contents of the registry are:

```
+-------+-----------------------------------------------------------+
| Value | Description                                               |
+=======+===========================================================+
|     0 | Natively Signed C509 Certificate following X.509 v3       |
+-------+-----------------------------------------------------------+
|     1 | CBOR re-encoding of X.509 v3 Certificate                  |
+-------+-----------------------------------------------------------+
```

Figure 6: C509 Certificate Types
11.2. C509 Attributes Registry

IANA has created a new registry titled "C509 Attributes" under the new heading "CBOR Encoded X509 Certificates (C509 Certificates)". The columns of the registry are Value, Name, Identifiers, OID, DER, Comments, and Reference, where Value is an non-negative integer, and the other columns are text strings. For values in the interval [0, 23] the registration procedure is "IETF Review" and "Expert Review". For all other values the registration procedure is "Expert Review". The initial contents of the registry are:
<table>
<thead>
<tr>
<th>Value</th>
<th>Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Email Address</td>
</tr>
<tr>
<td></td>
<td>emailAddress, e-mailAddress</td>
</tr>
<tr>
<td></td>
<td>1.2.840.113549.1.9.1</td>
</tr>
<tr>
<td></td>
<td>06 09 2A 86 86 F7 0D 01 09 01</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Common Name</td>
</tr>
<tr>
<td></td>
<td>commonName, cn</td>
</tr>
<tr>
<td></td>
<td>2.5.4.3</td>
</tr>
<tr>
<td></td>
<td>06 03 55 04 03</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Surname</td>
</tr>
<tr>
<td></td>
<td>surname, sn</td>
</tr>
<tr>
<td></td>
<td>2.5.4.4</td>
</tr>
<tr>
<td></td>
<td>06 03 55 04 04</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Serial Number</td>
</tr>
<tr>
<td></td>
<td>serialNumber</td>
</tr>
<tr>
<td></td>
<td>2.5.4.5</td>
</tr>
<tr>
<td></td>
<td>06 03 55 04 05</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Country</td>
</tr>
<tr>
<td></td>
<td>countryName, c</td>
</tr>
<tr>
<td></td>
<td>2.5.4.6</td>
</tr>
<tr>
<td></td>
<td>06 03 55 04 06</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Locality</td>
</tr>
<tr>
<td></td>
<td>localityName, locality, l</td>
</tr>
<tr>
<td></td>
<td>2.5.4.7</td>
</tr>
<tr>
<td></td>
<td>06 03 55 04 07</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>State or Province</td>
</tr>
<tr>
<td></td>
<td>stateOrProvinceName, st</td>
</tr>
<tr>
<td></td>
<td>2.5.4.8</td>
</tr>
<tr>
<td></td>
<td>06 03 55 04 08</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Street Address</td>
</tr>
<tr>
<td></td>
<td>streetAddress, street</td>
</tr>
<tr>
<td></td>
<td>2.5.4.9</td>
</tr>
<tr>
<td></td>
<td>06 03 55 04 09</td>
</tr>
</tbody>
</table>
8 | Name: Organization
| Identifiers: organizationName, o
| OID: 2.5.4.10
| DER: 06 03 55 04 0A
| Comments:

9 | Name: Organizational Unit
| Identifiers: organizationalUnitName, ou
| OID: 2.5.4.11
| DER: 06 03 55 04 0B
| Comments:

10 | Name: Title
| Identifiers: title
| OID: 2.5.4.12
| DER: 06 03 55 04 0C
| Comments:

11 | Name: Business Category
| Identifiers: businessCategory
| OID: 2.5.4.15
| DER: 06 03 55 04 0F
| Comments:

12 | Name: Postal Code
| Identifiers: postalCode
| OID: 2.5.4.17
| DER: 06 03 55 04 11
| Comments:

13 | Name: Given Name
| Identifiers: givenName
| OID: 2.5.4.42
| DER: 06 03 55 04 2A
| Comments:

14 | Name: Initials
| Identifiers: initials
| OID: 2.5.4.43
| DER: 06 03 55 04 2B
| Comments:

15 | Name: Generation Qualifier
| Identifiers: generationQualifier
| OID: 2.5.4.44
| DER: 06 03 55 04 2C
| Comments:
<table>
<thead>
<tr>
<th></th>
<th>Name:</th>
<th>DN Qualifier</th>
<th>Identifiers:</th>
<th>dnQualifier</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>OID:</td>
<td>2.5.4.46</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DER:</td>
<td>06 03 55 04 2E</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Name:</td>
<td>Pseudonym</td>
<td>Identifiers:</td>
<td>pseudonym</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>OID:</td>
<td>2.5.4.65</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DER:</td>
<td>06 03 55 04 41</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Name:</td>
<td>Organization Identifier</td>
<td>Identifiers:</td>
<td>organizationIdentifier</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>OID:</td>
<td>2.5.4.97</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DER:</td>
<td>06 03 55 04 61</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Name:</td>
<td>Inc. Locality</td>
<td>Identifiers:</td>
<td>jurisdictionOfIncorporationLocalityName</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>OID:</td>
<td>1.3.6.1.4.1.311.60.2.1.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DER:</td>
<td>06 0B 2B 06 01 04 01 82 37 3C 02 01 01</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Name:</td>
<td>Inc. State or Province</td>
<td>Identifiers:</td>
<td>jurisdictionOfIncorporation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>StateOrProvinceName</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>OID:</td>
<td>1.3.6.1.4.1.311.60.2.1.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DER:</td>
<td>06 0B 2B 06 01 04 01 82 37 3C 02 01 02</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Name:</td>
<td>Inc. Country</td>
<td>Identifiers:</td>
<td>jurisdictionOfIncorporationCountryName</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>OID:</td>
<td>1.3.6.1.4.1.311.60.2.1.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DER:</td>
<td>06 0B 2B 06 01 04 01 82 37 3C 02 01 03</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Name:</td>
<td>Domain Component</td>
<td>Identifiers:</td>
<td>domainComponent, dc</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>OID:</td>
<td>0.9.2342.19200300.100.1.25</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DER:</td>
<td>06 0A 09 92 26 89 93 F2 2C 64 01 19</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
11.3. C509 Extensions Registry

IANA has created a new registry titled "C509 Extensions Registry" under the new heading "CBOR Encoded X509 Certificates (C509 Certificates)". The columns of the registry are Value, Name, Identifiers, OID, DER, Comments, extensionValue, and Reference, where Value is a positive integer, and the other columns are text strings. For values in the interval [1, 23] the registration procedure is "IETF Review" and "Expert Review". For all other values the registration procedure is "Expert Review". The initial contents of the registry are:
<table>
<thead>
<tr>
<th>Value</th>
<th>Extension</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>-----------</td>
</tr>
<tr>
<td>1</td>
<td>Name: Subject Key Identifier</td>
</tr>
<tr>
<td></td>
<td>Identifiers: subjectKeyIdentifier</td>
</tr>
<tr>
<td></td>
<td>OID: 2.5.29.14</td>
</tr>
<tr>
<td></td>
<td>DER: 06 03 55 1D 0E</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
</tr>
<tr>
<td></td>
<td>extensionValue: SubjectKeyIdentifier</td>
</tr>
<tr>
<td>2</td>
<td>Name: Key Usage</td>
</tr>
<tr>
<td></td>
<td>Identifiers: keyUsage</td>
</tr>
<tr>
<td></td>
<td>OID: 2.5.29.15</td>
</tr>
<tr>
<td></td>
<td>DER: 06 03 55 1D 0F</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
</tr>
<tr>
<td></td>
<td>AttributeValue: KeyUsage</td>
</tr>
<tr>
<td>3</td>
<td>Name: Subject Alternative Name</td>
</tr>
<tr>
<td></td>
<td>Identifiers: subjectAltName</td>
</tr>
<tr>
<td></td>
<td>OID: 2.5.29.17</td>
</tr>
<tr>
<td></td>
<td>DER: 06 03 55 1D 11</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
</tr>
<tr>
<td></td>
<td>extensionValue: SubjectAltName</td>
</tr>
<tr>
<td>4</td>
<td>Name: Basic Constraints</td>
</tr>
<tr>
<td></td>
<td>Identifiers: basicConstraints</td>
</tr>
<tr>
<td></td>
<td>OID: 2.5.29.19</td>
</tr>
<tr>
<td></td>
<td>DER: 06 03 55 1D 13</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
</tr>
<tr>
<td></td>
<td>extensionValue: BasicConstraints</td>
</tr>
<tr>
<td>5</td>
<td>Name: CRL Distribution Points</td>
</tr>
<tr>
<td></td>
<td>Identifiers: cRLDistributionPoints</td>
</tr>
<tr>
<td></td>
<td>OID: 2.5.29.31</td>
</tr>
<tr>
<td></td>
<td>DER: 06 03 55 1D 1F</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
</tr>
<tr>
<td></td>
<td>extensionValue: CRLDistributionPoints</td>
</tr>
<tr>
<td>6</td>
<td>Name: Certificate Policies</td>
</tr>
<tr>
<td></td>
<td>Identifiers: certificatePolicies</td>
</tr>
<tr>
<td></td>
<td>OID: 2.5.29.32</td>
</tr>
<tr>
<td></td>
<td>DER: 06 03 55 1D 20</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
</tr>
<tr>
<td></td>
<td>extensionValue: CertificatePolicies</td>
</tr>
<tr>
<td>7</td>
<td>Name: Authority Key Identifier</td>
</tr>
<tr>
<td></td>
<td>Identifiers: authorityKeyIdentifier</td>
</tr>
<tr>
<td></td>
<td>OID: 2.5.29.35</td>
</tr>
<tr>
<td></td>
<td>DER: 06 03 55 1D 23</td>
</tr>
<tr>
<td>Name:</td>
<td>Extension Value:</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Extended Key Usage</td>
<td>AuthorityKeyIdentifier</td>
</tr>
<tr>
<td>Authority Information Access</td>
<td>AuthorityInfoAccessSyntax</td>
</tr>
<tr>
<td>Signed Certificate Timestamp List</td>
<td>SignedCertificateTimestamps</td>
</tr>
<tr>
<td>Subject Directory Attributes</td>
<td>SubjectDirectoryAttributes</td>
</tr>
<tr>
<td>Issuer Alternative Name</td>
<td>IssuerAltName</td>
</tr>
<tr>
<td>Name Constraints</td>
<td>NameConstraints</td>
</tr>
<tr>
<td>Policy Mappings</td>
<td>PolicyMappings</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
</tr>
<tr>
<td>---</td>
<td>-----------</td>
</tr>
<tr>
<td>28</td>
<td>Name: Policy Constraints</td>
</tr>
<tr>
<td>29</td>
<td>Name: Freshest CRL</td>
</tr>
<tr>
<td>30</td>
<td>Name: Inhibit anyPolicy</td>
</tr>
<tr>
<td>31</td>
<td>Name: Subject Information Access</td>
</tr>
<tr>
<td>32</td>
<td>Name: IP Resources</td>
</tr>
<tr>
<td>33</td>
<td>Name: AS Resources</td>
</tr>
<tr>
<td>34</td>
<td>Name: IP Resources v2</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
</tr>
<tr>
<td>---</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>extensionValue: IPAddrBlocks</td>
</tr>
<tr>
<td>---</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>35</td>
<td>Name: AS Resources v2</td>
</tr>
<tr>
<td></td>
<td>Identifiers: autonomousSysIds-v2</td>
</tr>
<tr>
<td></td>
<td>OID: 1.3.6.1.5.5.7.1.29</td>
</tr>
<tr>
<td></td>
<td>DER: 06 08 2B 06 01 05 05 07 01 1D</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
</tr>
<tr>
<td></td>
<td>extensionValue: ASIdentifiers</td>
</tr>
<tr>
<td>---</td>
<td>---------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
11.4. C509 Certificate Policies Registry

IANA has created a new registry titled "C509 Certificate Policies Registry" under the new heading "CBOR Encoded X509 Certificates (C509 Certificates)". The columns of the registry are Value, Name, Identifiers, OID, DER, Comments, and Reference, where Value is an integer, and the other columns are text strings. For values in the interval [-24, 23] the registration procedure is "IETF Review" and "Expert Review". For all other values the registration procedure is "Expert Review". The initial contents of the registry are:
<table>
<thead>
<tr>
<th>Value</th>
<th>Certificate Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Name: Any Policy</td>
</tr>
<tr>
<td></td>
<td>Identifiers: anyPolicy</td>
</tr>
<tr>
<td></td>
<td>OID: 2.5.29.32.0</td>
</tr>
<tr>
<td></td>
<td>DER: 06 04 55 1D 20 00</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
</tr>
<tr>
<td>1</td>
<td>Name: Domain Validation (DV)</td>
</tr>
<tr>
<td></td>
<td>Identifiers: domain-validated</td>
</tr>
<tr>
<td></td>
<td>OID: 2.23.140.1.2.1</td>
</tr>
<tr>
<td></td>
<td>DER: 06 06 67 81 0C 01 02 01</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
</tr>
<tr>
<td>2</td>
<td>Name: Organization Validation (OV)</td>
</tr>
<tr>
<td></td>
<td>Identifiers: organization-validated</td>
</tr>
<tr>
<td></td>
<td>OID: 2.23.140.1.2.2</td>
</tr>
<tr>
<td></td>
<td>DER: 06 06 67 81 0C 01 02 02</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
</tr>
<tr>
<td>3</td>
<td>Name: Individual Validation (IV)</td>
</tr>
<tr>
<td></td>
<td>Identifiers: individual-validated</td>
</tr>
<tr>
<td></td>
<td>OID: 2.23.140.1.2.3</td>
</tr>
<tr>
<td></td>
<td>DER: 06 06 67 81 0C 01 02 03</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
</tr>
<tr>
<td>4</td>
<td>Name: Extended Validation (EV)</td>
</tr>
<tr>
<td></td>
<td>Identifiers: ev-guidelines</td>
</tr>
<tr>
<td></td>
<td>OID: 2.23.140.1.1</td>
</tr>
<tr>
<td></td>
<td>DER: 06 05 67 81 0C 01 01</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
</tr>
<tr>
<td>7</td>
<td>Name: Resource PKI (RPKI)</td>
</tr>
<tr>
<td></td>
<td>Identifiers: id-cp-ipAddr-asNumber</td>
</tr>
<tr>
<td></td>
<td>OID: 1.3.6.1.5.5.7.14.2</td>
</tr>
<tr>
<td></td>
<td>DER: 06 08 2B 06 01 05 05 07 0E 02</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
</tr>
<tr>
<td>8</td>
<td>Name: Resource PKI (RPKI) (Alternative)</td>
</tr>
<tr>
<td></td>
<td>Identifiers: id-cp-ipAddr-asNumber-v2</td>
</tr>
<tr>
<td></td>
<td>OID: 1.3.6.1.5.5.7.14.3</td>
</tr>
<tr>
<td></td>
<td>DER: 06 08 2B 06 01 05 05 07 0E 03</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
</tr>
<tr>
<td>10</td>
<td>Name: Remote SIM Provisioning Role</td>
</tr>
<tr>
<td></td>
<td>Certificate Issuer</td>
</tr>
<tr>
<td></td>
<td>Identifiers: id-rspRole-ci</td>
</tr>
<tr>
<td></td>
<td>OID: 2.23.146.1.2.1.0</td>
</tr>
<tr>
<td></td>
<td>DER:       06 07 67 81 12 01 02 01 00</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
</tr>
<tr>
<td>11</td>
<td>Name:     Remote SIM Provisioning Role</td>
</tr>
<tr>
<td></td>
<td>eUICC</td>
</tr>
<tr>
<td></td>
<td>Identifiers: id-rspRole-euicc</td>
</tr>
<tr>
<td></td>
<td>OID: 2.23.146.1.2.1.1</td>
</tr>
<tr>
<td></td>
<td>DER: 06 07 67 81 12 01 02 01 01</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
</tr>
<tr>
<td>12</td>
<td>Name:     Remote SIM Provisioning Role</td>
</tr>
<tr>
<td></td>
<td>eUICC Manufacturer</td>
</tr>
<tr>
<td></td>
<td>Identifiers: id-rspRole-eum</td>
</tr>
<tr>
<td></td>
<td>OID: 2.23.146.1.2.1.2</td>
</tr>
<tr>
<td></td>
<td>DER: 06 07 67 81 12 01 02 01 02</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
</tr>
<tr>
<td>13</td>
<td>Name:     Remote SIM Provisioning Role</td>
</tr>
<tr>
<td></td>
<td>SM-DP+ TLS</td>
</tr>
<tr>
<td></td>
<td>Identifiers: id-rspRole-dp-tls</td>
</tr>
<tr>
<td></td>
<td>OID: 2.23.146.1.2.1.3</td>
</tr>
<tr>
<td></td>
<td>DER: 06 07 67 81 12 01 02 01 03</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
</tr>
<tr>
<td>14</td>
<td>Name:     Remote SIM Provisioning Role</td>
</tr>
<tr>
<td></td>
<td>SM-DP+ Authentication</td>
</tr>
<tr>
<td></td>
<td>Identifiers: id-rspRole-dp-auth</td>
</tr>
<tr>
<td></td>
<td>OID: 2.23.146.1.2.1.4</td>
</tr>
<tr>
<td></td>
<td>DER: 06 07 67 81 12 01 02 01 04</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
</tr>
<tr>
<td>15</td>
<td>Name:     Remote SIM Provisioning Role</td>
</tr>
<tr>
<td></td>
<td>SM-DP+ Profile Binding</td>
</tr>
<tr>
<td></td>
<td>Identifiers: id-rspRole-dp-pb</td>
</tr>
<tr>
<td></td>
<td>OID: 2.23.146.1.2.1.5</td>
</tr>
<tr>
<td></td>
<td>DER: 06 07 67 81 12 01 02 01 05</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
</tr>
<tr>
<td>16</td>
<td>Name:     Remote SIM Provisioning Role</td>
</tr>
<tr>
<td></td>
<td>SM-DS TLS</td>
</tr>
<tr>
<td></td>
<td>Identifiers: id-rspRole-ds-tls</td>
</tr>
<tr>
<td></td>
<td>OID: 2.23.146.1.2.1.6</td>
</tr>
<tr>
<td></td>
<td>DER: 06 07 67 81 12 01 02 01 06</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
</tr>
<tr>
<td>17</td>
<td>Name:     Remote SIM Provisioning Role</td>
</tr>
<tr>
<td></td>
<td>SM-DS Authentication</td>
</tr>
<tr>
<td></td>
<td>Identifiers: id-rspRole-ds-auth</td>
</tr>
<tr>
<td></td>
<td>OID: 2.23.146.1.2.1.7</td>
</tr>
</tbody>
</table>
11.5. C509 Policies Qualifiers Registry

IANA has created a new registry titled "C509 Policies Qualifiers Registry" under the new heading "CBOR Encoded X509 Certificates (C509 Certificates)". The columns of the registry are Value, Name, Identifiers, OID, DER, Comments, and Reference, where Value is an integer, and the other columns are text strings. For values in the interval [-24, 23] the registration procedure is "IETF Review" and "Expert Review". For all other values the registration procedure is "Expert Review". The initial contents of the registry are:

<table>
<thead>
<tr>
<th>Value</th>
<th>Certificate Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>-------------------</td>
</tr>
<tr>
<td></td>
<td>Certificate Policy</td>
</tr>
<tr>
<td>1</td>
<td>Name: Certification Practice Statement</td>
</tr>
<tr>
<td></td>
<td>Identifiers: id-qt-cps, cps</td>
</tr>
<tr>
<td></td>
<td>OID: 1.3.6.1.5.5.7.2.1</td>
</tr>
<tr>
<td></td>
<td>DER: 06 08 2B 06 01 05 05 07 02 01</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
</tr>
<tr>
<td>2</td>
<td>Name: User Notice</td>
</tr>
<tr>
<td></td>
<td>Identifiers: id-qt-unotice, unotice</td>
</tr>
<tr>
<td></td>
<td>OID: 1.3.6.1.5.5.7.2.2</td>
</tr>
<tr>
<td></td>
<td>DER: 06 08 2B 06 01 05 05 07 02 02</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
</tr>
</tbody>
</table>

11.6. C509 Information Access Registry

IANA has created a new registry titled "C509 Information Access Registry" under the new heading "CBOR Encoded X509 Certificates (C509 Certificates)". The columns of the registry are Value, Name, Identifiers, OID, DER, Comments, and Reference, where Value is an integer, and the other columns are text strings. For values in the interval [-24, 23] the registration procedure is "IETF Review" and "Expert Review". For all other values the registration procedure is "Expert Review". The initial contents of the registry are:
<table>
<thead>
<tr>
<th>Value</th>
<th>Information Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>+-------+-----------------------------------------------------------+</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Name: OCSP</td>
</tr>
<tr>
<td></td>
<td>Identifiers: id-ad-ocsp, id-pkix-ocsp</td>
</tr>
<tr>
<td></td>
<td>OID: 1.3.6.1.5.5.7.48.1</td>
</tr>
<tr>
<td></td>
<td>DER: 06 08 2B 06 01 05 05 07 30 01</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
</tr>
<tr>
<td>2</td>
<td>Name: CA Issuers</td>
</tr>
<tr>
<td></td>
<td>Identifiers: id-ad-caIssuers, caIssuers</td>
</tr>
<tr>
<td></td>
<td>OID: 1.3.6.1.5.5.7.48.2</td>
</tr>
<tr>
<td></td>
<td>DER: 06 08 2B 06 01 05 05 07 30 02</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
</tr>
<tr>
<td>3</td>
<td>Name: Time Stamping</td>
</tr>
<tr>
<td></td>
<td>Identifiers: id-ad-timeStamping, timeStamping</td>
</tr>
<tr>
<td></td>
<td>OID: 1.3.6.1.5.5.7.48.3</td>
</tr>
<tr>
<td></td>
<td>DER: 06 08 2B 06 01 05 05 07 30 03</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
</tr>
<tr>
<td>5</td>
<td>Name: CA Repository</td>
</tr>
<tr>
<td></td>
<td>Identifiers: id-ad-caRepository</td>
</tr>
<tr>
<td></td>
<td>OID: 1.3.6.1.5.5.7.48.5</td>
</tr>
<tr>
<td></td>
<td>DER: 06 08 2B 06 01 05 05 07 30 05</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
</tr>
<tr>
<td>10</td>
<td>Name: RPKI Manifest</td>
</tr>
<tr>
<td></td>
<td>Identifiers: id-ad-rpkiManifest</td>
</tr>
<tr>
<td></td>
<td>OID: 1.3.6.1.5.5.7.48.10</td>
</tr>
<tr>
<td></td>
<td>DER: 06 08 2B 06 01 05 05 07 30 0A</td>
</tr>
<tr>
<td></td>
<td>Comments: RFC 6487</td>
</tr>
<tr>
<td>11</td>
<td>Name: Signed Object</td>
</tr>
<tr>
<td></td>
<td>Identifiers: id-ad-signedObject</td>
</tr>
<tr>
<td></td>
<td>OID: 1.3.6.1.5.5.7.48.11</td>
</tr>
<tr>
<td></td>
<td>DER: 06 08 2B 06 01 05 05 07 30 0B</td>
</tr>
<tr>
<td></td>
<td>Comments: RFC 6487</td>
</tr>
<tr>
<td>13</td>
<td>Name: RPKI Notify</td>
</tr>
<tr>
<td></td>
<td>Identifiers: id-ad-rpkiNotify</td>
</tr>
<tr>
<td></td>
<td>OID: 1.3.6.1.5.5.7.48.13</td>
</tr>
<tr>
<td></td>
<td>DER: 06 08 2B 06 01 05 05 07 30 0D</td>
</tr>
<tr>
<td></td>
<td>Comments: RFC 8182</td>
</tr>
</tbody>
</table>

Figure 11: C509 Information Accesses
11.7. C509 Extended Key Usages Registry

IANA has created a new registry titled "C509 Extended Key Usages Registry" under the new heading "CBOR Encoded X509 Certificates (C509 Certificates)". The columns of the registry are Value, Name, Identifiers, OID, DER, Comments, and Reference, where Value is an integer, and the other columns are text strings. For values in the interval [-24, 23] the registration procedure is "IETF Review" and "Expert Review". For all other values the registration procedure is "Expert Review". The initial contents of the registry are:
<table>
<thead>
<tr>
<th>Value</th>
<th>Extended Key Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Name: Any Extended Key Usage</td>
</tr>
<tr>
<td></td>
<td>Identifiers: anyExtendedKeyUsage</td>
</tr>
<tr>
<td></td>
<td>OID: 2.5.29.37.0</td>
</tr>
<tr>
<td></td>
<td>DER: 06 04 55 1D 25 00</td>
</tr>
<tr>
<td></td>
<td>Comments: RFC 5280</td>
</tr>
<tr>
<td>1</td>
<td>Name: TLS Server authentication</td>
</tr>
<tr>
<td></td>
<td>Identifiers: id-kp-serverAuth</td>
</tr>
<tr>
<td></td>
<td>OID: 1.3.6.1.5.5.7.3.1</td>
</tr>
<tr>
<td></td>
<td>DER: 06 08 2B 06 01 05 05 07 03 01</td>
</tr>
<tr>
<td></td>
<td>Comments: RFC 5280</td>
</tr>
<tr>
<td>2</td>
<td>Name: TLS Client Authentication</td>
</tr>
<tr>
<td></td>
<td>Identifiers: id-kp-clientAuth</td>
</tr>
<tr>
<td></td>
<td>OID: 1.3.6.1.5.5.7.3.2</td>
</tr>
<tr>
<td></td>
<td>DER: 06 08 2B 06 01 05 05 07 03 02</td>
</tr>
<tr>
<td></td>
<td>Comments: RFC 5280</td>
</tr>
<tr>
<td>3</td>
<td>Name: Code Signing</td>
</tr>
<tr>
<td></td>
<td>Identifiers: id-kp-codeSigning</td>
</tr>
<tr>
<td></td>
<td>OID: 1.3.6.1.5.5.7.3.3</td>
</tr>
<tr>
<td></td>
<td>DER: 06 08 2B 06 01 05 05 07 03 03</td>
</tr>
<tr>
<td></td>
<td>Comments: RFC 5280</td>
</tr>
<tr>
<td>4</td>
<td>Name: Email protection (S/MIME)</td>
</tr>
<tr>
<td></td>
<td>Identifiers: id-kp-emailProtection</td>
</tr>
<tr>
<td></td>
<td>OID: 1.3.6.1.5.5.7.3.4</td>
</tr>
<tr>
<td></td>
<td>DER: 06 08 2B 06 01 05 05 07 03 04</td>
</tr>
<tr>
<td></td>
<td>Comments: RFC 5280</td>
</tr>
<tr>
<td>8</td>
<td>Name: Time Stamping</td>
</tr>
<tr>
<td></td>
<td>Identifiers: id-kp-timeStamping, timestamping</td>
</tr>
<tr>
<td></td>
<td>OID: 1.3.6.1.5.5.7.3.8</td>
</tr>
<tr>
<td></td>
<td>DER: 06 08 2B 06 01 05 05 07 03 08</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
</tr>
<tr>
<td>9</td>
<td>Name: OCSP Signing</td>
</tr>
<tr>
<td></td>
<td>Identifiers: id-kp-OCSPSigning</td>
</tr>
<tr>
<td></td>
<td>OID: 1.3.6.1.5.5.7.3.9</td>
</tr>
<tr>
<td></td>
<td>DER: 06 08 2B 06 01 05 05 07 03 09</td>
</tr>
<tr>
<td></td>
<td>Comments: RFC 5280</td>
</tr>
<tr>
<td>10</td>
<td>Name: Kerberos PKINIT Client Auth</td>
</tr>
<tr>
<td></td>
<td>Identifiers: id-pkinit-KPClientAuth</td>
</tr>
<tr>
<td></td>
<td>OID: 1.3.6.1.5.2.3.4</td>
</tr>
<tr>
<td></td>
<td>DER: 06 07 2B 06 01 05 02 03 04</td>
</tr>
<tr>
<td>11</td>
<td>Name: Kerberos PKINIT KDC</td>
</tr>
<tr>
<td>----</td>
<td>----------------------------</td>
</tr>
<tr>
<td></td>
<td>Identifiers: id-pkinit-KPKdc</td>
</tr>
<tr>
<td></td>
<td>OID: 1.3.6.1.5.2.3.5</td>
</tr>
<tr>
<td></td>
<td>DER: 06 07 2B 06 01 05 02 03 05</td>
</tr>
<tr>
<td></td>
<td>Comments: RFC 4556</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>12</th>
<th>Name: SSH Client</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Identifiers: id-kp-secureShellClient</td>
</tr>
<tr>
<td></td>
<td>OID: 1.3.6.1.5.5.7.3.21</td>
</tr>
<tr>
<td></td>
<td>DER: 06 08 2B 06 01 05 05 07 03 15</td>
</tr>
<tr>
<td></td>
<td>Comments: RFC 6187</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>13</th>
<th>Name: Kerberos PKINIT KDC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Identifiers: id-pkinit-KPKdc</td>
</tr>
<tr>
<td></td>
<td>OID: 1.3.6.1.5.5.7.3.22</td>
</tr>
<tr>
<td></td>
<td>DER: 06 08 2B 06 01 05 05 07 03 16</td>
</tr>
<tr>
<td></td>
<td>Comments: RFC 6187</td>
</tr>
</tbody>
</table>

**Comments:**
- RFC 4556
- RFC 6187
11.8. C509 General Names Registry

IANA has created a new registry titled "C509 General Names Registry" under the new heading "CBOR Encoded X509 Certificates (C509 Certificates)". The columns of the registry are Value, General Name, and Reference, where Value is an integer, and the other columns are text strings. For values in the interval [-24, 23] the registration procedure is "IETF Review" and "Expert Review". For all other values the registration procedure is "Expert Review". The initial contents of the registry are:
<table>
<thead>
<tr>
<th>Value</th>
<th>General Names</th>
</tr>
</thead>
<tbody>
<tr>
<td>-2</td>
<td>Name: otherName with SmtpUTF8Mailbox</td>
</tr>
<tr>
<td></td>
<td>Comments: id-on-SmtpUTF8Mailbox</td>
</tr>
<tr>
<td></td>
<td>(1.3.6.1.5.5.7.8.9)</td>
</tr>
<tr>
<td></td>
<td>06 08 2B 06 01 05 05 07 08 09</td>
</tr>
<tr>
<td></td>
<td>Value: text</td>
</tr>
<tr>
<td>-1</td>
<td>Name: otherName with hardwareModuleName</td>
</tr>
<tr>
<td></td>
<td>Comments: id-on-hardwareModuleNamee</td>
</tr>
<tr>
<td></td>
<td>(1.3.6.1.5.5.7.8.4)</td>
</tr>
<tr>
<td></td>
<td>06 08 2B 06 01 05 05 07 08 04</td>
</tr>
<tr>
<td></td>
<td>Value: [ ~oid, bytes ]</td>
</tr>
<tr>
<td>0</td>
<td>Name: otherName</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
</tr>
<tr>
<td></td>
<td>Value: [ ~oid, bytes ]</td>
</tr>
<tr>
<td>1</td>
<td>Name: rfc822Name</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
</tr>
<tr>
<td></td>
<td>Value: text</td>
</tr>
<tr>
<td>2</td>
<td>Name: dNSName</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
</tr>
<tr>
<td></td>
<td>Value: text</td>
</tr>
<tr>
<td>4</td>
<td>Name: directoryName</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
</tr>
<tr>
<td></td>
<td>Value: Name</td>
</tr>
<tr>
<td>6</td>
<td>Name: uniformResourceIdentifier</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
</tr>
<tr>
<td></td>
<td>Value: text</td>
</tr>
<tr>
<td>7</td>
<td>Name: iPAddress</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
</tr>
<tr>
<td></td>
<td>Value: bytes</td>
</tr>
<tr>
<td>8</td>
<td>Name: registeredID</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
</tr>
<tr>
<td></td>
<td>Value: ~oid</td>
</tr>
</tbody>
</table>

Figure 13: C509 General Names
11.9. C509 Signature Algorithms Registry

IANA has created a new registry titled "C509 Signature Algorithms" under the new heading "CBOR Encoded X509 Certificates (C509 Certificates)". The columns of the registry are Value, Name, Identifiers, OID, Parameters, DER, Comments, and Reference, where Value is an integer, and the other columns are text strings. For values in the interval [-24, 23] the registration procedure is "IETF Review" and "Expert Review". For all other values the registration procedure is "Expert Review". The initial contents of the registry are:
<table>
<thead>
<tr>
<th>Value</th>
<th>X.509 Signature Algorithms</th>
</tr>
</thead>
<tbody>
<tr>
<td>-256</td>
<td>Name: RSASSA-PKCS1-v1_5 with SHA-1</td>
</tr>
<tr>
<td></td>
<td>Identifiers: sha1-with-rsa-signature,</td>
</tr>
<tr>
<td></td>
<td>sha1WithRSAEncryption,</td>
</tr>
<tr>
<td></td>
<td>sha-1WithRSAEncryption</td>
</tr>
<tr>
<td></td>
<td>OID: 1.2.840.113549.1.1.5</td>
</tr>
<tr>
<td></td>
<td>Parameters: NULL</td>
</tr>
<tr>
<td></td>
<td>DER: 30 0D 06 09 2A 86 48 86 F7 0D 01 01 05 05 00</td>
</tr>
<tr>
<td></td>
<td>Comments: Don't use</td>
</tr>
<tr>
<td>-255</td>
<td>Name: ECDSA with SHA-1</td>
</tr>
<tr>
<td></td>
<td>Identifiers: ecdsa-with-SHA1</td>
</tr>
<tr>
<td></td>
<td>OID: 1.2.840.10045.4.1</td>
</tr>
<tr>
<td></td>
<td>Parameters: Absent</td>
</tr>
<tr>
<td></td>
<td>DER: 30 09 06 07 2A 86 48 CE 3D 04 01</td>
</tr>
<tr>
<td></td>
<td>Comments: Don't use. Compressed signature value</td>
</tr>
<tr>
<td>0</td>
<td>Name: ECDSA with SHA-256</td>
</tr>
<tr>
<td></td>
<td>Identifiers: ecdsa-with-SHA256</td>
</tr>
<tr>
<td></td>
<td>OID: 1.2.840.10045.4.3.2</td>
</tr>
<tr>
<td></td>
<td>Parameters: Absent</td>
</tr>
<tr>
<td></td>
<td>DER: 30 0A 06 08 2A 86 48 CE 3D 04 03 02</td>
</tr>
<tr>
<td></td>
<td>Comments: Compressed signature value</td>
</tr>
<tr>
<td>1</td>
<td>Name: ECDSA with SHA-384</td>
</tr>
<tr>
<td></td>
<td>Identifiers: ecdsa-with-SHA384</td>
</tr>
<tr>
<td></td>
<td>OID: 1.2.840.10045.4.3.3</td>
</tr>
<tr>
<td></td>
<td>Parameters: Absent</td>
</tr>
<tr>
<td></td>
<td>DER: 30 0A 06 08 2A 86 48 CE 3D 04 03 03</td>
</tr>
<tr>
<td></td>
<td>Comments: Compressed signature value</td>
</tr>
<tr>
<td>2</td>
<td>Name: ECDSA with SHA-512</td>
</tr>
<tr>
<td></td>
<td>Identifiers: ecdsa-with-SHA512</td>
</tr>
<tr>
<td></td>
<td>OID: 1.2.840.10045.4.3.4</td>
</tr>
<tr>
<td></td>
<td>Parameters: Absent</td>
</tr>
<tr>
<td></td>
<td>DER: 30 0A 06 08 2A 86 48 CE 3D 04 03 04</td>
</tr>
<tr>
<td></td>
<td>Comments: Compressed signature value</td>
</tr>
<tr>
<td>3</td>
<td>Name: ECDSA with SHAKE128</td>
</tr>
<tr>
<td></td>
<td>Identifiers: id-ecdsa-with-shake128</td>
</tr>
<tr>
<td></td>
<td>OID: 1.3.6.1.5.5.7.6.32</td>
</tr>
<tr>
<td></td>
<td>Parameters: Absent</td>
</tr>
<tr>
<td></td>
<td>DER: 30 0A 06 08 2B 06 01 05 05 07 06 20</td>
</tr>
<tr>
<td></td>
<td>Comments: Compressed signature value</td>
</tr>
<tr>
<td>4</td>
<td>Name: ECDSA with SHAKE256</td>
</tr>
<tr>
<td></td>
<td>Identifiers: id-ecdsa-with-shake256</td>
</tr>
<tr>
<td>OID: 1.3.6.1.5.5.7.6.33</td>
<td>Parameters: Absent</td>
</tr>
</tbody>
</table>

| Name: Ed25519 | Identifiers: id-Ed25519, id-EdDSA25519 | OID: 1.3.101.112 | Parameters: Absent | DER: 30 05 06 03 2B 65 70 | Comments: |

| Name: Ed448 | Identifiers: id-Ed448, id-EdDSA448 | OID: 1.3.101.113 | Parameters: Absent | DER: 30 05 06 03 2B 65 71 | Comments: |

| Name: RSASSA-PKCS1-v1_5 with SHA-256 | Identifiers: sha256WithRSAEncryption | OID: 1.2.840.113549.1.1.11 | Parameters: NULL | DER: 30 0B 06 09 2A 86 48 86 F7 0D 01 01 0B 05 00 | Comments: |

| Name: RSASSA-PKCS1-v1_5 with SHA-384 | Identifiers: sha384WithRSAEncryption | OID: 1.2.840.113549.1.1.12 | Parameters: NULL | DER: 30 0B 06 09 2A 86 48 86 F7 0D 01 01 0C 05 00 | Comments: |

| Name: RSASSA-PKCS1-v1_5 with SHA-512 | Identifiers: sha512WithRSAEncryption | OID: 1.2.840.113549.1.1.13 | Parameters: NULL | DER: 30 0B 06 09 2A 86 48 86 F7 0D 01 01 0D 05 00 | Comments: |

<p>| Name: RSASSA-PSS with SHA-256 | Identifiers: rsa-a-pss, id-RSASSA-PSS | OID: 1.2.840.113549.1.1.10 | Parameters: SHA-256, MGF-1 with SHA-256, saltLength = 32 | DER: 30 41 06 09 2A 86 48 86 F7 0D 01 01 0A 30 34 | A0 0F 30 0D 06 09 60 86 48 01 65 03 04 02 01 | 05 00 A1 1C 30 1A 06 09 2A 86 48 86 F7 0D 01 | 01 08 30 0D 06 09 60 86 48 01 65 03 04 02 01 | 05 00 a2 03 02 01 20 | Comments: |</p>
<table>
<thead>
<tr>
<th></th>
<th>Name: RSASSA-PSS with SHA-384</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>27</td>
<td>Identifiers: rsassa-pss, id-RSASSA-PSS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>OID: 1.2.840.113549.1.1.10</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Parameters: SHA-384, MGF-1 with SHA-384, saltLength = 48</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DER: 30 41 06 09 2A 86 48 86 F7 0D 01 01 0A 30 34</td>
<td></td>
</tr>
<tr>
<td></td>
<td>A0 0F 30 0D 06 09 60 86 48 01 65 03 04 02 02</td>
<td></td>
</tr>
<tr>
<td></td>
<td>05 00 A1 1C 30 1A 06 09 2A 86 48 86 F7 0D 01</td>
<td></td>
</tr>
<tr>
<td></td>
<td>01 08 30 0D 06 09 60 86 48 01 65 03 04 02 02</td>
<td></td>
</tr>
<tr>
<td></td>
<td>05 00 A2 03 02 01 30</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
<td></td>
</tr>
</tbody>
</table>

|   | Name: RSASSA-PSS with SHA-512 |   |
| 28 | Identifiers: rsassa-pss, id-RSASSA-PSS |   |
|   | OID: 1.2.840.113549.1.1.10 |   |
|   | Parameters: SHA-512, MGF-1 with SHA-512, saltLength = 64 |   |
|   | DER: 30 41 06 09 2A 86 48 86 F7 0D 01 01 0A 30 34 |   |
|   | A0 0F 30 0D 06 09 60 86 48 01 65 03 04 02 03 |   |
|   | 05 00 A1 1C 30 1A 06 09 2A 86 48 86 F7 0D 01 |   |
|   | 01 08 30 0D 06 09 60 86 48 01 65 03 04 02 03 |   |
|   | 05 00 A2 03 02 01 40 |   |
|   | Comments: |   |

|   | Name: RSASSA-PSS with SHAKE128 |   |
| 29 | Identifiers: id-RSASSA-PSS-SHAKE128 |   |
|   | OID: 1.3.6.1.5.5.5.1.30 |   |
|   | Parameters: Absent |   |
|   | DER: 30 0A 06 08 2B 06 01 05 05 07 06 1E |   |
|   | Comments: |   |

|   | Name: RSASSA-PSS with SHAKE256 |   |
| 30 | Identifiers: id-RSASSA-PSS-SHAKE256 |   |
|   | OID: 1.3.6.1.5.5.5.31 |   |
|   | Parameters: Absent |   |
|   | DER: 30 0A 06 08 2B 06 01 05 05 07 06 1F |   |
|   | Comments: |   |

|   | Name: HSS / LMS |   |
| 42 | Identifiers: id-alg-hss-lms-hashsig, id-alg-mts-hashsig |   |
|   | OID: 1.2.840.113549.1.9.16.3.17 |   |
|   | Parameters: Absent |   |
|   | DER: 30 0D 06 0B 2A 86 48 86 F7 0D 01 09 10 03 11 |   |
|   | Comments: |   |

|   | Name: XMSS |   |
| 43 | Identifiers: id_alg_xmss |   |
|   | OID: 0.4.0.127.0.15.1.13.0 |   |
|   | Parameters: Absent |   |
| Name: XMSS^MT |
| Identifiers: id_alg_xmssmt |
| OID: 0.4.0.127.0.15.1.1.14.0 |
| Parameters: Absent |
| DER: 30 0B 06 09 04 00 7F 00 0F 01 01 0E 00 |
| Comments: |
11.10. C509 Public Key Algorithms Registry

IANA has created a new registry titled "C509 Public Key Algorithms" under the new heading "CBOR Encoded X509 Certificates (C509 Certificates)". The columns of the registry are Value, Name, Identifiers, OID, Parameters, DER, Comments, and Reference, where Value is an integer, and the other columns are text strings. For values in the interval [-24, 23] the registration procedure is "IETF Review" and "Expert Review". For all other values the registration procedure is "Expert Review". The initial contents of the registry are:
<table>
<thead>
<tr>
<th>Value</th>
<th>X.509 Public Key Algorithms</th>
</tr>
</thead>
</table>

0 | Name: RSA |
| | Identifiers: rsaEncryption |
| | OID: 1.2.840.113549.1.1.1 |
| | Parameters: NULL |
| | DER: 30 0d 06 09 2a 86 48 86 f7 0d 01 01 01 05 00 |
| | Comments: Compressed subjectPublicKey |

1 | Name: EC Public Key (Weierstraß) with secp256r1 |
| | Identifiers: ecPublicKey, id-ecPublicKey |
| | OID: 1.2.840.10045.2.1 |
| | Parameters: namedCurve = secp256r1 (1.2.840.10045.3.1.7) |
| | DER: 30 13 06 07 2a 86 48 ce 3d 02 01 06 08 2a 86 |
| | 48 ce 3d 03 01 07 |
| | Comments: Point compressed subjectPublicKey |
| | Also known as P-256, ansip256r1, prime256v1 |

2 | Name: EC Public Key (Weierstraß) with secp384r1 |
| | Identifiers: ecPublicKey, id-ecPublicKey |
| | OID: 1.2.840.10045.2.1 |
| | Parameters: namedCurve = secp384r1 (1.3.132.0.34) |
| | DER: 30 10 06 07 2a 86 48 ce 3d 02 01 06 05 2b 81 |
| | 04 00 22 |
| | Comments: Point compressed subjectPublicKey |
| | Also known as P-384, ansip384r1 |

3 | Name: EC Public Key (Weierstraß) with secp521r1 |
| | Identifiers: ecPublicKey, id-ecPublicKey |
| | OID: 1.2.840.10045.2.1 |
| | Parameters: namedCurve = secp521r1 (1.3.132.0.35) |
| | DER: 30 10 06 07 2a 86 48 ce 3d 02 01 06 05 2b 81 |
| | 04 00 23 |
| | Comments: Point compressed subjectPublicKey |
| | Also known as P-521, ansip521r1 |

8 | Name: X25519 (Montgomery) |
| | Identifiers: id-X25519 |
| | OID: 1.3.101.110 |
| | Parameters: Absent |
| | DER: 30 05 06 03 2b 65 6e |
| | Comments: |

9 | Name: X448 (Montgomery) |
| | Identifiers: id-X448 |
| | OID: 1.3.101.111 |
| | Parameters: Absent |
| | DER: 30 05 06 03 2b 65 6f |
10 | Name: Ed25519 (Twisted Edwards) |
| Identifiers: id-Ed25519, id-EdDSA25519 |
| OID: 1.3.101.112 |
| Parameters: Absent |
| DER: 30 05 06 03 2B 65 70 |

11 | Name: Ed448 (Edwards) |
| Identifiers: id-Ed448, id-EdDSA448 |
| OID: 1.3.101.113 |
| Parameters: Absent |
| DER: 30 05 06 03 2B 65 71 |

16 | Name: HSS / LMS |
| Identifiers: id-alg-hss-lms-hashsig, id-alg-mts-hashsig |
| OID: 1.2.840.113549.1.9.16.3.17 |
| Parameters: Absent |
| DER: 30 0D 06 0B 2A 86 48 86 F7 0D 01 09 10 03 11 |

17 | Name: XMSS |
| Identifiers: id_alg_xmss |
| OID: 0.4.0.127.0.15.1.1.13.0 |
| Parameters: Absent |
| DER: 30 0B 06 09 04 00 7F 00 0F 01 01 0D 00 |

18 | Name: XMSS^MT |
| Identifiers: id_alg_xmssmt |
| OID: 0.4.0.127.0.15.1.1.14.0 |
| Parameters: Absent |
| DER: 30 0B 06 09 04 00 7F 00 0F 01 01 0E 00 |

24 | Name: EC Public Key (Weierstraß) with brainpoolP256r1 |
| Identifiers: ecPublicKey, id-ecPublicKey |
| OID: 1.2.840.10045.2.1 |
| Parameters: namedCurve = brainpoolP256r1 |
| DER: 30 13 06 07 2A 86 48 CE 3D 02 01 06 09 2B 24 |
| 03 03 02 08 01 01 07 |
| Comments: Point compressed subjectPublicKey |

25 | Name: EC Public Key (Weierstraß) with brainpoolP384r1 |
<table>
<thead>
<tr>
<th></th>
<th>Identifiers: ecPublicKey, id-ecPublicKey</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>OID: 1.2.840.10045.2.1</td>
</tr>
<tr>
<td></td>
<td>Parameters: namedCurve = brainpoolP384r1</td>
</tr>
<tr>
<td></td>
<td>(1.3.36.3.3.2.8.1.1.11)</td>
</tr>
<tr>
<td></td>
<td>DER: 30 13 06 07 2A 86 48 CE 3D 02 01 06 09 2B 24</td>
</tr>
<tr>
<td></td>
<td>Comments: Point compressed subjectPublicKey</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td>-----------------------------------------------------------</td>
</tr>
<tr>
<td>Name:</td>
<td>EC Public Key (Weierstraß) with</td>
</tr>
<tr>
<td>26</td>
<td>brainpoolP512r1</td>
</tr>
<tr>
<td></td>
<td>Identifiers: ecPublicKey, id-ecPublicKey</td>
</tr>
<tr>
<td></td>
<td>OID: 1.2.840.10045.2.1</td>
</tr>
<tr>
<td></td>
<td>Parameters: namedCurve = brainpoolP512r1</td>
</tr>
<tr>
<td></td>
<td>(1.3.36.3.3.2.8.1.1.13)</td>
</tr>
<tr>
<td></td>
<td>DER: 30 13 06 07 2A 86 48 CE 3D 02 01 06 09 2B 24</td>
</tr>
<tr>
<td></td>
<td>Comments: Point compressed subjectPublicKey</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td>-----------------------------------------------------------</td>
</tr>
<tr>
<td>Name:</td>
<td>EC Public Key (Weierstraß) with</td>
</tr>
<tr>
<td>27</td>
<td>FRP256v1</td>
</tr>
<tr>
<td></td>
<td>Identifiers: ecPublicKey, id-ecPublicKey</td>
</tr>
<tr>
<td></td>
<td>OID: 1.2.840.10045.2.1</td>
</tr>
<tr>
<td></td>
<td>Parameters: namedCurve = FRP256v1</td>
</tr>
<tr>
<td></td>
<td>(1.2.250.1.223.101.256.1)</td>
</tr>
<tr>
<td></td>
<td>DER: 30 13 06 07 2A 86 48 CE 3D 02 01 06 0A 2A 81</td>
</tr>
<tr>
<td></td>
<td>7A 01 81 5F 65 82 00 01</td>
</tr>
<tr>
<td></td>
<td>Comments: Point compressed subjectPublicKey</td>
</tr>
</tbody>
</table>
11.11. COSE Header Parameters Registry

EDITORS NOTE: The text should be moved a section and not be in the IANA Section.

This document registers the following entries in the "COSE Header Parameters" registry under the "CBOR Object Signing and Encryption (COSE)" heading. The formatting and processing for c5b, c5c, and c5t, and c5u are similar to x5bag, x5chain, x5t, x5u defined in [I-D.ietf-cose-x509] except that the certificates are C509 instead of DER encoded X.509 and uses a COSE_C509 structure instead of COSE_X509. c5u provides an alternative way to identify an untrusted certificate bag/chain by reference with a URI. The content is a COSE_C509 item served with the application/cbor content format. The COSE_C509 structure used in c5b, c5c, and c5u is defined as:

\[
\text{COSE\_C509} = \text{C509Certificate} / [\text{2* C509Certificate}] 
\]

As the contents of c5bag, c5chain, c5t, and c5u are untrusted input, the header parameters can be in either the protected or unprotected header bucket. The trust mechanism MUST process any certificates in the c5b, c5c, and c5u parameters as untrusted input. The presence of a self-signed certificate in the parameter MUST NOT cause the update of the set of trust anchors without some out-of-band confirmation.

Note that certificates can also be identified with a 'kid' header parameter by storing 'kid' and the associated bag or chain in a dictionary.

+-----------+-------+----------------+------------------------------+
<table>
<thead>
<tr>
<th>Name</th>
<th>Label</th>
<th>Value Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>c5b</td>
<td>TBD1</td>
<td>COSE_C509</td>
<td>An unordered bag of C509</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>certificates</td>
</tr>
<tr>
<td>c5c</td>
<td>TBD2</td>
<td>COSE_C509</td>
<td>An ordered chain of C509</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>certificates</td>
</tr>
<tr>
<td>c5t</td>
<td>TBD3</td>
<td>COSE_CertHash</td>
<td>Hash of a C509Certificate</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c5u</td>
<td>TBD4</td>
<td>uri</td>
<td>URI pointing to a COSE_C509</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>containing a ordered chain</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>of certificates</td>
</tr>
</tbody>
</table>
|-----------+-------+----------------+------------------------------+
11.12. TLS Certificate Types Registry

This document registers the following entry in the "TLS Certificate Types" registry under the "Transport Layer Security (TLS) Extensions" heading. The new certificate type can be used with additional TLS certificate compression [RFC8879]. C509 is defined in the same way as as X509, but uses a different value and instead of DER-encoded X.509 certificate, opaque cert_data<1..2^24-1> contains a the CBOR sequence ~C509Certificate (an unwrapped C509Certificate).

EDITOR'S NOTE: The TLS registrations should be discussed and approved by the TLS WG at a later stage. When COSE WG has adopted work on C509 certificates, it could perhaps be presented in the TLS WG. The TLS WG might e.g. want a separate draft in the TLS WG.

+-------------------+-------------------+-------------------+-------------------+
| Value             | Name              | Recommended       | Comment           |
| TBD5              | C509 Certificate  | Y                 |                   |
+-------------------+-------------------+-------------------+-------------------+

11.13. CBOR Tags Registry

This document registers the following entries in the "CBOR Tags" registry under the "Concise Binary Object Representation (CBOR) Tags" heading.

+---------------------+-------------------------------------------------+
| Tag                  | X.509 Public Key Algorithms                      |
| TDB6                 | Data Item: COSE_C509                             |
|                     | Semantics: An ordered chain of C509 certificates  |
|                     | Reference: This document                         |
+---------------------+-------------------------------------------------+

12. References

12.1. Normative References


12.2. Informative References


[CAB-Code]


Appendix A. Example C509 Certificates

A.1. Example RFC 7925 profiled X.509 Certificate

Example of [RFC7925] profiled X.509 certificate parsed with OpenSSL.

Certificate:
Data:
  Version: 3 (0x2)
  Serial Number: 128269 (0x1f50d)
  Signature Algorithm: ecdsa-with-SHA256
  Issuer: CN=RFC test CA
  Validity
    Not Before: Jan 1 00:00:00 2020 GMT
    Not After: Feb 2 00:00:00 2021 GMT
  Subject: CN=01-23-45-FF-FE-67-89-AB
  Subject Public Key Info:
    Public Key Algorithm: id-ecPublicKey
    Public-Key: (256 bit)
    pub:
      3f:16:21:3a:04:52:5e:d4:44:50:b1:01:9c:2d:fd:
      f7:79:2a:c2:06
    ASN1 OID: prime256v1
    NIST CURVE: P-256
X509v3 extensions:
  X509v3 Key Usage:
    Digital Signature
  Signature Algorithm: ecdsa-with-SHA256

The DER encoding of the above certificate is 314 bytes.
A.1.1. Example C509 Certificate Encoding

The CBOR encoding (~C509Certificate) of the same X.509 certificate is shown below in CBOR diagnostic format.

The size of the CBOR encoding (CBOR sequence) is 138 bytes.

```
30 82 01 36 30 81 DE A0 03 02 01 02 03 01 F5 0D 30 0A 06 08 2A 86
48 CE 3D 04 03 02 02 02 02 03 01 F5 0D 30 0A 06 08 2A 86
5A 17 0D 32 31 30 32 30 32 30 30 30 30 30 30 30 30 30 30 5A 30 22
31 20 30 30 30 30 30 30 5A 17 0D 32 31 30 31 2D 32 33 2D 34 35 2D
46 46 45 2D 36 37 2D 38 39 2D 41 42 30 59 30 13 06 07 2A 86 48 CE
3D 02 01 06 08 2A 86 48 CE 3D 03 01 07 03 42 00 04 B1 21 6A B9 6E
5B 3B 33 40 F5 BD F0 2E 69 3F 16 21 3A 04 52 5E D4 44 50 B1 01 9C
2D FD 38 38 AB AC 4E 14 D8 6C 09 83 ED 5E 9E EF 24 48 C6 86 1C
C4 06 54 71 77 E6 02 60 30 D0 51 F7 79 2A C2 06 A3 0F 30 0D 30 0B
06 03 55 1D 0F 04 04 03 02 07 80 30 0A 06 08 2A 86 48 CE 3D 04 03
02 03 47 00 30 44 02 20 44 5D 79 8C 90 E7 5F 00 DC 74 7A 65 4C
EC 6C FA 6F 03 72 76 E1 4E 52 ED 07 FC 16 29 4C 84 66 0D 02 20 5A
33 98 5D FB D4 BF DD 6D 4A CF 3B 04 C3 D4 6E BF 3B 7F A6 26 40
67 4F C0 35 4F A0 56 DB AE A6

A.1.1. Example C509 Certificate Encoding

The CBOR encoding (~C509Certificate) of the same X.509 certificate is shown below in CBOR diagnostic format.

/This defines a CBOR Sequence (RFC 8742):

```
1,
  h'01f50d,'
  "RFC test CA",
  1577836800,
  161224000,
  h'0123456789AB',
  1,
  h'02B1216A8096E5B3B3340F5BDF02E693F16213A04525ED44450
    B1019C2DFD3838AB',
  1,
  0,
  h'455D98C90E7F500DC747A654CEC6CFA6F037276E14E52ED07
    FC16294C8466D5A33985DFBD44FDD6D4ACF3804C3D46EBFB3B
    7FA6264674FC0354FA056DBAE6A6'

The size of the CBOR encoding (CBOR sequence) is 138 bytes.
A.1.2. Example: Natively Signed C509 Certificate

The corresponding natively signed C509 certificate in CBOR diagnostic format is identical, except for c509CertificateType and signatureValue.

/This defines a CBOR Sequence (RFC 8742):/

0,  
'01f50d',  
"RFC test CA",  
1577836800,  
161224000,  
'0123456789AB',  
1,  
'02B116AB964B3330F5B6E02E693F16213A04525ED4445B1019C2DFD3838AB',  
1,  
0,  
'B27A0B78B1455F71B68290F6C9A897F109F8B6C5957953BC67268AB0E4DDE99D273E04E4715383AB2257C6AAA35284E5ED18BDB91247E9F2C433136480B9'

The size of the CBOR encoding (CBOR sequence) is 138 bytes.
A.1.3. Example: Additional Keys for the Example Certificates

Below are the issuer key pair and the subject private key belonging to the above example certificates. The private keys are encoded as in COSE [RFC8152]. These issuer key pair can be used to sign or verify the example certificates and the subject private key allows the example certificates to be used in test vectors for other protocols like EDHOC.

issuerPublicKeyAlgorithm :
1 (EC Public Key (Weierstraß) with secp256r1)

issuerPublicKey :
h'02AE4CDB01F614DEFC7121285FDC7F5C6D1D42C95647F061BA0080DF678867845E'

issuerPrivateKey :
h'DC66B3415456D649429B53223DF7532B942D6B0E0842C30BCA4C0ACF91547BB2'

subjectPrivateKey :
h'D718111F3F9BD91B92FF6877F386BDBFCEA7154268FD7F2FB56EE17D99EA16D4'

A.2. Example IEEE 802.1AR profiled X.509 Certificate

EDITOR'S NOTE: To do

A.3. Example CAB Baseline ECDSA HTTPS X.509 Certificate

The www.ietf.org HTTPS server replies with a certificate message with 2 certificates. The DER encoding of the first certificate is 1209 bytes.
A.3.1. Example C509 Certificate Encoding

The CBOR encoding (~C509Certificate) of the first X.509 certificate is shown below in CBOR diagnostic format.
This defines a CBOR Sequence (RFC 8742):

1,
h'047FA1E31928EE403BA0B83A395673FC',
[  
-4, "US",
-8, "Cloudflare, Inc.",
-1, "Cloudflare Inc ECC CA-3"
],
1595980800,
1627560000,
[  
-4, "US",
-6, "CA",
-5, "San Francisco",
-8, "Cloudflare, Inc.",
-1, "sni.cloudflaressl.com"
],
1,
h'03963ECDD84DCD1B93A1CF432D1A7217D6C63BDE3355A02F8CFB5AD8994CD44E20',
[  
7, h'5CE37EAEBB0750E946788B445FAD9241087961F',
1, h'CC0B50E7D837DBF243F3853D4860F53B39BE9B2A',
-2, 1,
8, [1, 2],
   "http://crl4.digicert.com/CloudflareIncECCCA-3.crl"],
6, [h'6086480186FD6C0101', [1, "https://www.digicert.com/CPS"], 2],
9, [1, "http://ocsp.digicert.com",
   2, "http://cacerts.digicert.com/CloudflareIncECCCA-3.crt"],
-4, -2,
10, [
 h'F65C942FD1773022145418083094568EE34D131933BFDF0C2F200BCC4EF164E3',
  77922190,
  0,
 h'F81B4A93D2F0D4C4176DFB488BCC73B86443D7DE0E6AC8174D8948A8843668
  29FF5A34068A240C69502788E8EE25AB7ED2BCBF686ECE7B5F96B431A90702FA',
 h'5CDC4392FFEE6AB4544B15E9AD456E61037FBD5FA47DCA17394B25EE6F6C70ECA',
  77922238,
  0,
 h'891C197FBF0E3D30CB6CEE60D94C3C75FD1175336931108D89812D4D29D81D0
  A159D16C4647D1483757FC6DE4E75EC7B5EF657EFE028F8E5CC4792682D4C43'    
  ]
],
0,
h'BD63CF4F7E5CF66C29385EA71CFBFC1E3F7B1CD07251A221F77769C0F471DFEA
 B5C06CC45854FA30B2828B1D3BB9A6661ED5031725B1A8202E0DA5B9F95402'
The size of the CBOR encoding (CBOR sequence) is 783 bytes.

A.4. Example CAB Baseline RSA HTTPS X.509 Certificate

The tools.ietf.org HTTPS server replies with a certificate message with 4 certificates. The DER encoding of the first certificate is 1647 bytes.
A.4.1. Example C509 Certificate Encoding

The CBOR encoding (~C509Certificate) of the first X.509 certificate is shown below in CBOR diagnostic format.
This defines a CBOR Sequence (RFC 8742):

1, h'6A55C870E39B40E',
[ -4, "US",
  -6, "Arizona",
  -5, "Scottsdale",
  -8, "Starfield Technologies, Inc.",
  -9, "http://certs.starfieldtech.com/repository/",
  -1, "Starfield Secure Certificate Authority - G2"
], 1601581116, 1635881916,
[ -9, "Domain Control Validated",
  1, "*.tools.ietf.org"
], 0, h'B1E137E8EB82D689FADB5C24B77F02C4ADE726E3E1366D1A8661EC4AD3D3260 E5F09985F47A485521EE0E3912FC6956CF56961C704E6E0F1D3B1E508879 3A0E314116F1B1026468A5CDF5A9A7C99F3508C37E275DD909CCFE3728AF37 D8B67BDD37EAE6977F7CA694ECCD06DF5D279B3B12E76FE086527B8211 7C72B346E5C1878B80F60CBE1EBDBD64458DC8359B2A6625BDC81B836E397E79 B2A9538A6008CB4A2A13393113B2CCF870CFA883D01A388AE12803611D2E4 2BDD79D8530126ED284FC98694834EC8E1142E85B3AF46EDD6946AF41250E7A AD8BF292CA79D97B324FF777E8F9B44F235CD45C03AED8AB3ACA135F5D5D5A1',
[ -4, -2, 8, [ 1, 2 ],
  -2, 5,
  5, ["http://crl.starfieldtech.com/sfig2s1-242.crl"],
  -2, 5,
  6, [ h'6086480186fd6e016071701',
    [1, "http://certificates.starfieldtech.com/repository/", 1 ],
  9, [ 1, "http://ocsp.starfieldtech.com/",
    2, "http://certificates.starfieldtech.com/repository/sfig2.crt" ],
  7, h'254581685026383D3B2D2CEBD6AD9B63DB36663',
  3, [ 2, "*.tools.ietf.org", 2, "tools.ietf.org" ],
  1, h'AD8AB41C0751D7928907B0B784622F36557A5F4D',
  10, [
    h'F65C942FD1773022145418083094568EE34D131933BFDF0C2F200BCC4EF164E3',
    1715,
    0,
    h'8CF54852CE5635439111CF10CDB91F52B33639223AD138A41DECA6FDE1E90F BCA2254366C19A2691C47A00B5663ABB4D42F8BAE6F4D2DAF2527CE6454995',
    h'5CDC4392FEE6AB34544B15E9ADB45661037FBD5FA47DCA17394B25EE6F6C70ECA',
    2012,
    0,
    h'A5E9096E63E914FDDEFF0352B91E50896007564B448A3828F596DC6B28726D
The size of the CBOR encoding (CBOR sequence) is 1245 bytes.

Acknowledgments

The authors want to thank Henk Birkholz, Carsten Bormann, Russ Housley, Olle Johansson, Benjamin Kaduk, Ilari Liusvaara, Laurence Lundblade, Francesca Palombinini, Thomas Peterson, Michael Richardson, Maik Reichert, Stefan Santesson, Jim Schaad, Fraser Tweedale, and Rene Struik for reviewing and commenting on intermediate versions of the draft and helping with GitHub.

Authors' Addresses

John Preuß Mattsson
Ericsson AB
Email: john.mattsson@ericsson.com

Göran Selander
Ericsson AB
Email: goran.selander@ericsson.com

Shahid Raza
RISE AB
Email: shahid.raza@ri.se

Joel Höglund
RISE AB
Email: joel.hoglund@ri.se

Martin Furuhed
Nexus Group
Email: martin.furuhed@nexusgroup.com