Internet Engineering Task Force (IETF)
Request for Comments: 5759
Category: Informational
ISSN: 2070-1721

J. Solinas
L. Zieglar
NSA

January 2010

Suite B Certificate and Certificate Revocation List (CRL) Profile

Abstract

This document specifies a base profile for X.509 v3 Certificates and X.509 v2 Certificate Revocation Lists (CRLs) for use with the United States National Security Agency's Suite B Cryptography. The reader is assumed to have familiarity with RFC 5280, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc5759.

Table of Contents

1. Introduction

This document specifies a base profile for X.509 v3 Certificates and X.509 v2 Certificate Revocation Lists (CRLs) for use by applications that support the United States National Security Agency's Suite B Cryptography.

The reader is assumed to have familiarity with [RFC5280]. This Suite B Certificate and CRL Profile is a profile of RFC 5280. All MUST-level requirements of RFC 5280 apply throughout this profile and are generally not repeated here. In cases where a MUST-level requirement is repeated for emphasis, the text notes the requirement is "in adherence with [RFC5280]". This profile contains changes that elevate some MAY-level options in RFC 5280 to SHOULD-level and MUST-level in this profile; this profile also contains changes that elevate some SHOULD-level options in RFC 5280 to MUST-level for this profile. All options from RFC 5280 that are not listed in this profile remain at the requirement level of RFC 5280.

The reader is also assumed to have familiarity with [RFC5480], which specifies the syntax and semantics for the Subject Public Key Information field in certificates that support Elliptic Curve Cryptography and [RFC5758], which specifies algorithm identifiers for Elliptic Curve Digital Signature Algorithm (ECDSA).

2. Conventions Used in This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. Requirements and Assumptions

The goal of this document is to define a base set of certificate and CRL formats to support interoperability among Suite B solutions. Specific communities, such as the US National Security Systems, may define community profiles that further restrict certificate and CRL formats by mandating the presence of extensions that are optional in this base profile, defining new optional or critical extension types, or restricting the values and/or presence of fields within existing extensions. However, communications between distinct communities MUST use the formats specified in this document when interoperability is desired. (Applications may add additional non-critical extensions to these formats but they MUST NOT assume that a remote peer will be able to process them.)

3.1. Implementing Suite B

Every Suite B certificate MUST use the X.509 v3 format, and contain either:

* An ECDSA-capable signing key, using curve P-256 or P-384; or

* An ECDH-capable (Elliptic Curve Diffie-Hellman) key establishment key, using curve P-256 or P-384.

Every Suite B certificate and CRL MUST be signed using ECDSA. The signing Certification Authority's (CA's) key MUST be on the curve P-256 or P-384 if the certificate contains a key on the curve P-256. If the certificate contains a key on the curve P-384, the signing CA's key MUST be on the curve P-384. Any certificate and CRL MUST be hashed using SHA-256 or SHA-384, matched to the size of the signing CA's key.

3.2. Suite B Object Identifiers

The primary OID structure for Suite B is as follows per [X9.62], [SEC2], [RFC5480], and [RFC5758].

```
ansi-X9-62 OBJECT IDENTIFIER ::= {
   iso(1) member-body(2) us(840) 10045 }

certicom-arc OBJECT IDENTIFIER ::= {
   iso(1) identified-organization(3) certicom(132) }

id-ecPublicKey OBJECT IDENTIFIER ::= {
   ansi-X9-62 keyType(2) 1 }

secp256r1 OBJECT IDENTIFIER ::= {
   ansi-X9-62 curves(3) prime(1) 7 }

secp384r1 OBJECT IDENTIFIER ::= {
   certicom-arc curve(0) 34 }

id-ecSigType OBJECT IDENTIFIER ::= {
   ansi-X9-62 signatures(4) }

ecdsa-with-SHA256 OBJECT IDENTIFIER ::= {
   id-ecSigType ecdsa-with-SHA2(3) 2 }

ecdsa-with-SHA384 OBJECT IDENTIFIER ::= {
   id-ecSigType ecdsa-with-SHA2(3) 3 }
```

4. Suite B Certificate and Certificate Extensions Profile

This Suite B certificate profile is a profile of [RFC5280]. The changes in the requirements from RFC 5280 are listed here. Note that RFC 5280 has varying mandates for marking extensions as critical or non-critical. This profile changes some of those mandates for extensions that are included in Suite B certificates.

4.1. signatureAlgorithm

The two algorithm identifiers used by Suite B are: 1.2.840.10045.4.3.2 for ecdsa-with-SHA256 and 1.2.840.10045.4.3.3 for ecdsa-with-SHA384, as described in [RFC5758] AND [X9.62].

The parameters MUST be absent as per [RFC5758].

4.2. signatureValue

ECDSA digital signature generation is described in [FIPS186-3]. An ECDSA signature value is comprised of two unsigned integers, denoted as r and s. r and s MUST be represented as ASN.1 INTEGERs. If the high order bit of the unsigned integer is a 1, an octet with the value 0x00 MUST be prepended to the binary representation before encoding it as an ASN.1 INTEGER. Unsigned integers for the P-256 and P-384 curves can be a maximum of 32 and 48 bytes, respectively. Therefore, converting each r and s to an ASN.1 INTEGER will result in a maximum of 33 bytes for the P-256 curve and 49 bytes for the P-384 curve.

The ECDSA signatureValue in an X.509 certificate is encoded as a BIT STRING value of a DER-encoded SEQUENCE of the two INTEGERS. As per [RFC5480], the structure, included for convenience, is as follows:

```
ECDSA-Sig-Value ::= SEQUENCE {
    r  INTEGER,
    s  INTEGER
  }
```

For example, in a signature using P-256 and hex notation:

```
r=  52e3f7b7 27fba9e8 eddb1d08 3b75c188
    2517e6dc 63ded9c0 524f8f9a 45dc8661

s=  b8930438 de8d33bd ab12c3a2 bdad9795
    92a1fd65 76d1734c 3eb0af34 0456aef4

r represented as a DER-encoded INTEGER:
   022052e3 f7b727fb a9e8eddb 1d083b75
   c1882517 e6dc63de d9c0524f 8f9a45dc
   8661

s represented as a DER-encoded INTEGER:
   022100b8 930438de 8d33bdab 12c3a2bd
   ad979592 a1fd6576 d1734c3e b0af3404
   56aef4

Representation of SEQUENCE of r and s:
   30450220 52e3f7b7 27fba9e8 eddb1d08
   3b75c188 2517e6dc 63ded9c0 524f8f9a
   45dc8661 022100b8 930438de 8d33bdab
   12c3a2bd ad979592 a1fd6576 d1734c3e
   b0af3404 56aef4
```

```
Representation of resulting signatureValue:
   03480030 45022052 e3f7b727 fba9e8ed
   db1d083b 75c18825 17e6dc63 ded9c052
   4f8f9a45 dc866102 2100b893 0438de8d
   33bdab12 c3a2bdad 979592a1 fd6576d1
   734c3eb0 af340456 aef4
```

4.3. Version

For this profile, Version MUST be 3, which means the value MUST be set to 2.

4.4. SubjectPublicKeyInfo

For ECDSA signing keys and ECDH key agreement keys, the algorithm ID, id-ecPublicKey, MUST be used.

The parameters of the AlgorithmIdentifier in this field MUST use the namedCurve option. The specifiedCurve and implicitCurve options described in [RFC5480] MUST NOT be used. The namedCurve MUST be either the OID for secp256r1 (curve P-256) or secp384r1 (curve P-384) [RFC5480].

The elliptic curve public key, ECPoint, SHALL be the OCTET STRING representation of an elliptic curve point following the conversion routine in section 2.2 of [RFC5480] and sections 2.3.1 and 2.3.2 of [SEC1].

Suite B implementations MAY use either the uncompressed form or the compressed form of the elliptic curve point [RFC5480]. For interoperability purposes, all relying parties MUST be prepared to process the uncompressed form.

The elliptic curve public key (an ECPoint that is an OCTET STRING) is mapped to a subjectPublicKey (a BIT STRING) as follows: the most significant bit of the OCTET STRING becomes the most significant bit of the BIT STRING and the least significant bit of the OCTET STRING becomes the least significant bit of the BIT STRING [RFC5480].

An octet string representation of a P-256 uncompressed elliptic curve point:

```
046cc93a 2cdb0308 47fa0734 2bc8e130
4c77f04f 63557372 43f3a5d7 f51baa82
23d21ebf b87d9944 f7ec170d 64f9924e
9ce20e4d 361c2db5 f1d52257 4259edad
5e
```

A DER-encoded bit string representation of the subject public key:

```
03420004 6cc93a2c db030847 fa07342b
c8e1304c 77f04f63 55737243 f3a5d7f5
1baa8223 d21ebfb8 7d9944f7 ec170d64
f9924e9c e20e4d36 1c2db5f1 d5225742
59edad5e
```

A DER-encoded representation of the AlgorithmIdentifier:

```
30130607 2a8648ce 3d020106 082a8648
ce3d0301 07
```

A DER-encoded representation of the subjectPublicKeyInfo using the P-256 curve:

```
30593013 06072a86 48ce3d02 0106082a
8648ce3d 03010703 4200046c c93a2cdb
030847fa 07342bc8 e1304c77 f04f6355
737243f3 a5d7f51b aa8223d2 1ebfb87d
9944f7ec 170d64f9 924e9ce2 0e4d361c
2db5f1d5 22574259 edad5e
```

4.5. Certificate Extensions for Particular Types of Certificates

Different types of certificates in this profile have different required and recommended extensions. Those are listed in this section. Those extensions from RFC 5280 not explicitly listed in this profile remain at the requirement levels of RFC 5280.

4.5.1. Suite B Self-Signed CA Certificates

In adherence with [RFC5280], self-signed CA certificates in this profile MUST contain the subjectKeyIdentifier, keyUsage, and basicConstraints extensions.

The keyUsage extension MUST be marked as critical. The keyCertSign and cRLSign bits MUST be set. The digitalSignature and nonRepudiation bits MAY be set. All other bits MUST NOT be set.

In adherence with [RFC5280], the basicConstraints extension MUST be marked as critical. The cA boolean MUST be set to indicate that the subject is a CA and the pathLenConstraint MUST NOT be present.

4.5.2. Suite B Non-Self-Signed CA Certificates

Non-self-signed CA Certificates in this profile MUST contain the authorityKeyIdentifier, keyUsage, and basicConstraints extensions. If there is a policy to be asserted, then the certificatePolicies extension MUST be included.

The keyUsage extension MUST be marked as critical. The keyCertSign and CRLSign bits MUST be set. The digitalSignature and nonRepudiation bits MAY be set. All other bits MUST NOT be set.

In adherence with [RFC5280], the basicConstraints extension MUST be marked as critical. The cA boolean MUST be set to indicate that the subject is a CA and the pathLenConstraint subfield is OPTIONAL.

If a policy is asserted, the certificatePolicies extension MUST be marked as non-critical, MUST contain the OIDs for the applicable certificate policies and SHOULD NOT use the policyQualifiers option. If a policy is not asserted, the certificatePolicies extension MUST be omitted.

Relying party applications conforming to this profile MUST be prepared to process the policyMappings, policyConstraints, and inhibitAnyPolicy extensions, regardless of criticality, following the guidance in [RFC5280] when they appear in non-self-signed CA certificates.

4.5.3. Suite B End Entity Signature and Key Establishment Certificates

In adherence with [RFC5280], end entity certificates in this profile MUST contain the authorityKeyIdentifier and keyUsage extensions. If there is a policy to be asserted, then the certificatePolicies extension MUST be included. End entity certificates SHOULD contain the subjectKeyIdentifier extension.

The keyUsage extension MUST be marked as critical.

For end entity digital signature certificates, the keyUsage extension MUST be set for digitalSignature. The nonRepudiation bit MAY be set. All other bits in the keyUsage extension MUST NOT be set.

For end entity key establishment certificates, the keyUsage extension MUST BE set for keyAgreement. The encipherOnly or decipherOnly bit MAY be set. All other bits in the keyUsage extension MUST NOT be set.

If a policy is asserted, the certificatePolicies extension MUST be marked as non-critical, MUST contain the OIDs for the applicable certificate policies and SHOULD NOT use the policyQualifiers option. If a policy is not asserted, the certificatePolicies extension MUST be omitted.

5. Suite B CRL and CRL Extensions Profile

This Suite B CRL profile is a profile of [RFC5280]. There are changes in the requirements from [RFC5280] for the signatures on CRLs of this profile.

The signatures on CRLs in this profile MUST follow the same rules from this profile that apply to signatures in the certificates, see section 4.

6. Security Considerations

The security considerations in [RFC5280], [RFC5480], and [RFC5758] apply.

A single key pair SHOULD NOT be used for both signature and key establishment per [SP-800-57].

The Suite B algorithms provide significantly improved performance when compared to equivalent-strength cryptography that does not employ elliptic curve cryptography. Where performance has previously been an impediment, use of Suite B may permit employment of PKI-based cryptographic security mechanisms.

7. IANA Considerations

This document makes extensive use of object identifiers to register public key types, elliptic curves, and algorithms. Most of them are registered in the ANSI X9.62 arc with the exception of some of the curves, which are in the Certicom, Inc. arc (these curves have been adopted by ANSI and NIST). Extensions in certificates and CRLs are identified using the object identifiers defined in an arc delegated by IANA to the PKIX working group. No further action by IANA is necessary for this document or any anticipated updates.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008.

[RFC5480] Turner, S., Brown, D., Yiu, K., Housley, R., and T. Polk, "Elliptic Curve Cryptography Subject Public Key Information", RFC 5480, March 2009.

[RFC5758] Dang, Q., Santesson, S., Moriarty, K., Brown, D., and T. Polk, "Internet X.509 Public Key Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA", RFC 5758, January 2010.

8.2. Informative References

[FIPS186-3] "Digital Signature Standard (DSS)", June 2009.

[SEC1] Standards for Efficient Cryptography, "SEC1: Elliptic Curve Cryptography", September 2000.

[SEC2] Standards for Efficient Cryptography, "SEC 2: Recommended Elliptic Curve Domain Parameters", September 2000.

[SP-800-57] Barker, E., Barker, W., Burr, W., Polk, W. Smid, M., "NIST SP-800-57:Recommendation for Key Management-Part 1: General", March 2007.

[X9.62] ANS X9.62, "Public Key Cryptography for the Financial Services Industry; The Elliptic Curve Digital Signature Algorithm (ECDSA)", December 2005.

[X9.63] ANS X9.63, "Public Key Cryptography for the Financial Services Industry; Key Agreement and Key Transport Using Elliptic Curve Cryptography", December 2001.

Authors' Addresses

Jerome Solinas
National Information Assurance Research Laboratory
National Security Agency

EMail: jasolin@orion.ncsc.mil

Lydia Zieglar
National Information Assurance Research Laboratory
National Security Agency

EMail: llziegl@tycho.ncsc.mil