Network Working Group
Internet-Draft
Intended status: Informational
Expires: September 2, 2010

J. Schaad
Soaring Hawk Consulting
S. Turner
IECA, Inc.

March 1, 2010

Additional New ASN.1 Modules
draft-turner-additional-new-asn-00

Abstract

The Cryptographic Message Syntax (CMS) format, and many associated formats, are expressed using ASN.1. The current ASN.1 modules conform to the 1988 version of ASN.1. This document updates some auxiliary ASN.1 modules to conform to the 2002 version of ASN.1. There are no bits-on-the-wire changes to any of the formats; this is simply a change to the syntax.

Status of this Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on September 2, 2010.

Copyright Notice

1. Introduction

Some developers would like the IETF to use the latest version of ASN.1 in its standards. Most of the RFCs that relate to security protocols still use ASN.1 from the 1988 standard, which has been deprecated. This is particularly true for the standards that relate to PKIX, CMS, and S/MIME.

This document updates the following RFCs to use ASN.1 modules that conform to the 2002 version of ASN.1 [ASN1-2002].

RFC 4049, BinaryTime: An Alternate Format for Representing Date and Time in ASN.1 [RFC4049]

RFC 4073, Protecting Multiple Contents with the Cryptographic Message Syntax (CMS) [RFC4073]

RFC 5752, Multiple Signatures in Cryptographic Message Syntax (CMS) [RFC5752]

Note that some of the modules in this document get some of their definitions from places different than the modules in the original RFCs. The idea is that these modules, when combined with the modules in [I-D.ietf-pkix-new-asn1] and [I-D.ietf-smime-new-asn1] can stand on their own and do not need to import definitions from anywhere else.

1.1. Requirements Terminology

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].

2. ASN.1 Module RFC 4049

```
BinarySigningTimeModule-2009
      { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
        pkcs-9(9) smime(16) modules(0) TBD-1 }
DEFINITIONS IMPLICIT TAGS ::=
BEGIN
  IMPORTS

  -- From PKIX-CommonTypes-2009 [I-D.ietf-pkix-new-asn1]

  ATTRIBUTE
    FROM PKIX-CommonTypes-2009
      { iso(1) identified-organization(3) dod(6) internet(1)
        security(5) mechanisms(5) pkix(7) id-mod(0)
        id-mod-pkixCommon-02(57) }
 ;

 -- BinaryTime Definition

BinaryTime ::= INTEGER (0..MAX)

-- Signing Binary Time Attribute

aa-binarySigningTime ATTRIBUTE ::= {
    TYPE BinarySigningTime
    IDENTIFIED BY id-aa-binarySigningTime }

id-aa-binarySigningTime OBJECT IDENTIFIER ::= { iso(1)
```

```
    member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9)
    smime(16) aa(2) 46 }

BinarySigningTime ::= BinaryTime

END
```


3. ASN.1 Module RFC 4073

```
ContentCollectionModule-2009
  { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
    pkcs-9(9) smime(16) modules(0) TBD-2 }
DEFINITIONS IMPLICIT TAGS ::=
BEGIN
IMPORTS

-- From CryptographicMessageSyntax-2009 [I-D.ietf-smime-new-asn1]
  CONTENT-TYPE, Attribute, ContentInfo
   FROM CryptographicMessageSyntax-2009
    { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
      pkcs-9(9) smime(16) modules(0) cms-2001(14) }
;

-- Content Collection Content Type and Object Identifier

ct-ContentCollection CONTENT TYPE ::= {
  ContentCollection IDENTIFIED BY id-ct-contentCollection }

id-ct-contentCollection OBJECT IDENTIFIER ::= {
```

```
      iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9)
      smime(16) ct(1) 19 }

   ContentCollection ::= SEQUENCE SIZE (1..MAX) OF ContentInfo

   -- Content With Attributes Content Type and Object Identifier

   ct-ContentWithAttributes CONTENT TYPE ::= {
     { ContentWithAttributes IDENTIFIED BY id-ct-contentWithAttrs }

   id-ct-contentWithAttrs OBJECT IDENTIFIER ::= {
     iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9)
     smime(16) ct(1) 20 }

   ContentWithAttributes ::= SEQUENCE {
      content  ContentInfo,
      attrs    SEQUENCE SIZE (1..MAX) OF Attribute
                                              { ContentAttributes }

   ContentAttributes ATTRIBUTE ::= { ... }
   END
```


4. ASN.1 Module RFC 5752

```
  MultipleSignatures-2009
    { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9)
      smime(16) modules(0) TBD-3 }
  DEFINITIONS IMPLICIT TAGS ::=
  BEGIN
  -- EXPORTS All
  -- The types and values defined in this module are exported for use
  -- in the other ASN.1 modules.  Other applications may use them for
  -- their own purposes.

  IMPORTS

  -- Imports from PKIX-Common-Types-2009 [I-D.ietf-pkix-new-asn1]
```

```
  ATTRIBUTE
    FROM PKIX-CommonTypes-2009
      { iso(1) identified-organization(3) dod(6) internet(1)
        security(5) mechanisms(5) pkix(7) id-mod(0)
        id-mod-pkixCommon-02(57) }

  -- Imports from CryptographicMessageSyntax-2009 [I-D.ietf-smime-new-asn1]

  DigestAlgorithmIdentifier, SignatureAlgorithmIdentifier
    FROM CryptographicMessageSyntax-2009
    { iso(1) member-body(2) us(840) rsadsi(113549)
      pkcs(1) pkcs-9(9) smime(16) modules(0) id-mod-cms-2004-02(41) }

  -- Imports from ExtendedSecurityServices-2009 [I-D.ietf-smime-new-asn1]

  ESSCertIDv2
    FROM ExtendedSecurityServices-2009
    { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9)
      smime(16) modules(0) id-mod-ess-2006-02(42) }
  ;

  -- Section 3.0

  at-multipleSignatures ATTRIBUTE ::= {
    TYPE MultipleSignature
    IDENTIFIED BY id-aa-multipleSignatures }

  id-aa-multipleSignatures OBJECT IDENTIFIER ::= {
    iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9)
    id-aa(2) 51 }

  MultipleSignatures ::= SEQUENCE {
```



```
    bodyHashAlg     DigestAlgorithmIdentifier,
    signAlg         SignatureAlgorithmIdentifier,
    signAttrsHash   SignAttrsHash,
    cert            ESSCertIDv2 OPTIONAL }

  SignAttrsHash ::= SEQUENCE {
    algID            DigestAlgorithmIdentifier,
    hash             OCTET STRING }
```

```
END -- of MultipleSignatures-2008
```


5. Security Considerations

This document itself does not have any security considerations. The ASN.1 modules keep the same bits-on-the-wire as the modules that they replace.

6. IANA Considerations

None.

7. Normative References

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

[RFC4049] Housley, R., "BinaryTime: An Alternate Format for Representing Date and Time in ASN.1", RFC 4049, April 2005.

[RFC4073] Housley, R., "Protecting Multiple Contents with the Cryptographic Message Syntax (CMS)", RFC 4073, May 2005.

[RFC5752] Turner, S. and J. Schaad, "Multiple Signatures in Cryptographic Message Syntax (CMS)", RFC 5752, January 2010.

[I-D.ietf-smime-new-asn1] Hoffman, P. and J. Schaad, "New ASN.1 Modules for CMS and S/MIME", draft-ietf-smime-new-asn1-07 (work in progress), August 2009.

[I-D.ietf-pkix-new-asn1] Hoffman, P. and J. Schaad, "New ASN.1 Modules for PKIX", draft-ietf-pkix-new-asn1-07 (work in progress), August 2009.

[ASN1-2002] ITU-T, "ITU-T Recommendation X.680, X.681, X.682, and X.683", 2002.

Authors' Addresses

Jim Schaad
Soaring Hawk Consulting
PO Box 675
Gold Bar, WA 98251

Email: ietf@augustcellars.com

Sean Turner
IECA, Inc.
3057 Nutley Street, Suite 106
Fairfax, VA 22031

Email: turners@ieca.com