RFC 9169
New ASN.1 Modules for the Evidence Record Syntax (ERS)

Abstract
The Evidence Record Syntax (ERS) and the conventions for including these evidence records in the Server-based Certificate Validation Protocol (SCVP) are expressed using ASN.1. This document offers alternative ASN.1 modules that conform to the 2002 version of ASN.1 and employ the conventions adopted in RFCs 5911, 5912, and 6268. There are no bits-on-the-wire changes to any of the formats; this is simply a change to the ASN.1 syntax.

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 candidates for any level of Internet Standard; see Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9169.

Copyright Notice
Copyright (c) 2021 IETF Trust and the persons identified as the document authors. All rights reserved.

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

Table of Contents

1. Introduction
2. ASN.1 Module for RFC 4998
3. ASN.1 Module for RFC 5276
4. IANA Considerations
5. Security Considerations
6. References
   6.1. Normative References
   6.2. Informative References

Authors’ Addresses

1. Introduction

Some developers would like the IETF to use the latest version of ASN.1 in its standards. This document provides alternative ASN.1 modules to assist in that goal.

The Evidence Record Syntax (ERS) [RFC4998] provides two ASN.1 modules: one using the 1988 syntax [OLD-ASN1], which has been deprecated by the ITU-T, and another one using the newer syntax [NEW-ASN1], which continues to be maintained and enhanced. This document provides an alternative ASN.1 module that follows the conventions established in [RFC5055], [RFC5911], and [RFC5912].

In addition, [RFC5276] specifies the mechanism for conveying evidence records in the Server-based Certificate Validation Protocol (SCVP) [RFC5055]. There is only one ASN.1 module in [RFC5276], and it uses the 1988 syntax [OLD-ASN1]. This document provides an alternative ASN.1 module using the newer syntax [NEW-ASN1] and follows the conventions established in [RFC5055], [RFC5911], and [RFC5912]. Note that [RFC5912] already includes an alternative ASN.1 module for SCVP [RFC5055].

The original ASN.1 modules get some of their definitions from places outside the RFC series. Some of the referenced definitions are somewhat difficult to find. The alternative ASN.1 modules offered in this document stand on their own when combined with the modules in [RFC5055], [RFC5911], and [RFC5912].

The alternative ASN.1 modules produce the same bits on the wire as the original ones.
The alternative ASN.1 modules are informative; the original ones are normative.
2. **ASN.1 Module for RFC 4998**
ERS-2021

{ iso(1) identified-organization(3) dod(6) internet(1)
  security(5) mechanisms(5) ltans(11) id-mod(0)
  id-mod-ers(1) id-mod-ers-v2(2) }

DEFINITIONS IMPLICIT TAGS ::= BEGIN

EXPORTS ALL;

IMPORTS

ContentInfo
  FROM CryptographicMessageSyntax-2010 -- in [RFC6268]
  { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
    pkcs-9(9) smime(16) modules(0) id-mod-cms-2009(58) }

AlgorithmIdentifier{}, DIGEST-ALGORITHM
  FROM AlgorithmInformation-2009 -- in [RFC5912]
  { iso(1) identified-organization(3) dod(6) internet(1)
    security(5) mechanisms(5) pkix(7) id-mod(0)
    id-mod-algorithmInformation-02(58) }

AttributeSet{}, ATTRIBUTE
  FROM PKIX-CommonTypes-2009 -- in [RFC5912]
  { iso(1) identified-organization(3) dod(6) internet(1)
    security(5) mechanisms(5) pkix(7) id-mod(0)
    id-mod-pkixCommon-02(57) }

;

ltans OBJECT IDENTIFIER ::= { iso(1) identified-organization(3)
  dod(6) internet(1) security(5) mechanisms(5) ltans(11) }

EvidenceRecord ::= SEQUENCE {
  version INTEGER { v1(1) },
  digestAlgorithms SEQUENCE OF AlgorithmIdentifier
  {DIGEST-ALGORITHM, {...}},
  cryptoInfos [0] CryptoInfos OPTIONAL,
  encryptionInfo [1] EncryptionInfo OPTIONAL,
  archiveTimeStampSequence ArchiveTimeStampSequence }

CryptoInfos ::= SEQUENCE SIZE (1..MAX) OF Attribute

ArchiveTimeStamp ::= SEQUENCE {
  digestAlgorithm [0] AlgorithmIdentifier
  {DIGEST-ALGORITHM, {...}} OPTIONAL,
  attributes [1] Attributes OPTIONAL,
  reducedHashtree [2] SEQUENCE OF PartialHashtree OPTIONAL,
  timeStamp ContentInfo }

PartialHashtree ::= SEQUENCE OF OCTET STRING

Attributes ::= SET SIZE (1..MAX) OF Attribute

ArchiveTimeStampChain ::= SEQUENCE OF ArchiveTimeStamp
ArchiveTimeStampSequence ::= SEQUENCE OF ArchiveTimeStampChain

EncryptionInfo ::= SEQUENCE {
  encryptionInfoType  ENCINFO-TYPE.&id
     {{SupportedEncryptionAlgorithms}},
  encryptionInfoValue  ENCINFO-TYPE.&Type
     {{SupportedEncryptionAlgorithms}@encryptionInfoType} }

ENCINFO-TYPE ::= TYPE-IDENTIFIER

SupportedEncryptionAlgorithms ENCINFO-TYPE ::= { ... }

aa-er-internal ATTRIBUTE ::= {
  TYPE EvidenceRecord IDENTIFIED BY id-aa-er-internal }

id-aa-er-internal  OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9) smime(16) id-aa(2) 49 }

aa-er-external ATTRIBUTE ::= {
  TYPE EvidenceRecord IDENTIFIED BY id-aa-er-external }

id-aa-er-external  OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9) smime(16) id-aa(2) 50 }

ERSAttrSet ATTRIBUTE ::= { aa-er-internal | aa-er-external, ... }

Attribute ::= AttributeSet {{ERSAttrSet}}

END
3. **ASN.1 Module for RFC 5276**
LTANS-SCVP-EXTENSION-2021
{ iso(1) identified-organization(3) dod(6) internet(1)
  security(5) mechanisms(5) ltans(11) id-mod(0)
  id-mod-ers-scvp(5) id-mod-ers-scvp-v2(2) }

DEFINITIONS IMPLICIT TAGS ::= BEGIN

EXPORTS ALL;

IMPORTS
id-swb, CertBundle, WANT-BACK, AllWantBacks
FROM SCVP-2009 -- in [RFC5912]
{ iso(1) identified-organization(3) dod(6) internet(1)
  security(5) mechanisms(5) pkix(7) id-mod(0)
  id-mod-scvp-02(52) }

EvidenceRecord
FROM ERS-2021 -- in [RFC9169]
{ iso(1) identified-organization(3) dod(6) internet(1)
  security(5) mechanisms(5) ltans(11) id-mod(0)
  id-mod-ers(1) id-mod-ers-v2(2) }

EvidenceRecordWantBack ::= SEQUENCE {
  targetWantBack  WANT-BACK.&id ({ExpandedWantBacks}),
  evidenceRecord  EvidenceRecord OPTIONAL }

EvidenceRecordWantBacks ::= SEQUENCE SIZE (1..MAX) OF
  EvidenceRecordWantBack

EvidenceRecords ::= SEQUENCE SIZE (1..MAX) OF EvidenceRecord

ExpandedWantBacks WANT-BACK ::= { AllWantBacks |
  NewWantBacks |
  ERSWantBacks, ... }

NewWantBacks WANT-BACK ::= { swb-partial-cert-path, ... }

swb-partial-cert-path WANT-BACK ::= { CertBundle IDENTIFIED BY id-swb-partial-cert-path }

id-swb-partial-cert-path OBJECT IDENTIFIER ::= { id-swb 15 }

ERSWantBacks WANT-BACK ::= { swb-ers-pkc-cert |
  swb-ers-best-cert-path |
  swb-ers-partial-cert-path |
  swb-ers-revocation-info |
  swb-ers-all, ... }

swb-ers-pkc-cert WANT-BACK ::= { EvidenceRecord IDENTIFIED BY id-swb-ers-pkc-cert }

id-swb-ers-pkc-cert OBJECT IDENTIFIER ::= { id-swb 16 }
4. IANA Considerations

IANA has assigned two object identifiers from the "SMI Security for LTANS Module Identifier" registry to identify the two ASN.1 modules in this document.

The following object identifiers have been assigned:

<table>
<thead>
<tr>
<th>OID Value</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.5.5.11.0.1.2</td>
<td>id-mod-ers-v2</td>
<td>RFC 9169</td>
</tr>
<tr>
<td>1.3.6.1.5.5.11.0.5.2</td>
<td>id-mod-ers-scvp-v2</td>
<td>RFC 9169</td>
</tr>
</tbody>
</table>

Table 1: IANA Object Identifiers

5. Security Considerations

Please see the security considerations in [RFC4998] and [RFC5276]. This document makes no changes to the security considerations in those documents. The ASN.1 modules in this document preserve bits on the wire as the ASN.1 modules that they replace.

6. References

6.1. Normative References

[NEW-ASN1]
6.2. Informative References


6.2. Informative References


Authors' Addresses

Russ Housley  
Vigil Security, LLC  
516 Dranesville Road  
Herndon, VA 20170  
United States of America  
Email: housley@vigilsec.com
Carl Wallace
Red Hound Software, Inc.
5112 27th St. N
Arlington, VA 22207
United States of America
Email: carl@redhoundsoftware.com