Internet Engineering Task Force (IETF)
Request for Comments: 7036
Category: Informational
ISSN: 2070-1721

R. Housley
Vigil Security

October 2013

Object Identifier Registry for the Long-Term Archive and Notary Services (LTANS) Working Group

Abstract

When the Long-Term Archive and Notary Services (LTANS) working group was chartered, an object identifier arc was set aside for use by that working group. This document describes the object identifiers that were assigned, and it establishes IANA allocation policies for any future assignments within that arc.

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/rfc7036.

Table of Contents

1. Introduction

When the Long-Term Archive and Notary Services (LTANS) working group was chartered, an object identifier arc was set aside for use by that working group. These object identifiers are primarily used with Abstract Syntax Notation One (ASN.1) [ASN1-88] [ASN1-97].

The LTANS object identifier arc is:

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

This document describes the object identifiers that were assigned, and it establishes IANA allocation policies for any future assignments within that arc.

2. Subordinate Object Identifier Arcs

Three subordinate object identifier arcs were used. The first arc, id-mod, was used to assign ASN.1 module identifiers. The second arc, id-ct, was used to assign Cryptographic Message Syntax (CMS) content types. The third arc, id-em, was set aside for Evidence Record Syntax (ERS) encryption methods.

```
id-mod  OBJECT IDENTIFIER ::= { id-ltans 0 }
id-ct   OBJECT IDENTIFIER ::= { id-ltans 1 }
id-em   OBJECT IDENTIFIER ::= { id-ltans 2 }
```

3. Module Identifiers

The Evidence Record Syntax (ERS) [RFC4998] includes two ASN.1 modules. Both modules define the same syntax, but one module uses the 1997 ASN.1 syntax, and the other module uses the 1988 ASN.1 syntax. These module identifiers are:

```
id-mod-ers          OBJECT IDENTIFIER ::= { id-mod 1 }
id-mod-ers-v1       OBJECT IDENTIFIER ::= { id-mod 1 1 }
id-mod-ers88        OBJECT IDENTIFIER ::= { id-mod 2 }
id-mod-ers88-v1     OBJECT IDENTIFIER ::= { id-mod 2 1 }
```

The Long-term Archive Protocol (LTAP) [LTAP] includes two ASN.1 modules. While this protocol was never published as an RFC, the module identifiers were assigned to facilitate implementation. Both modules define the same syntax, but one module uses the 1997 ASN.1 syntax, and the other module uses the 1988 ASN.1 syntax. These module identifiers are:

```
id-mod-ltap88       OBJECT IDENTIFIER ::= { id-mod 3 }
id-mod-ltap88-v0    OBJECT IDENTIFIER ::= { id-mod 3 0 }
id-mod-ltap88-v1    OBJECT IDENTIFIER ::= { id-mod 3 1 }
id-mod-ltap         OBJECT IDENTIFIER ::= { id-mod 4 }
id-mod-ltap-v0      OBJECT IDENTIFIER ::= { id-mod 4 0 }
id-mod-ltap-v1      OBJECT IDENTIFIER ::= { id-mod 4 1 }
```

The document that describes the conventions for using the Server-Based Certificate Validation Protocol (SCVP) to convey Long-Term Evidence Records [RFC5276] includes one ASN.1 module. The module identifier is:

```
id-mod-ers-scvp     OBJECT IDENTIFIER ::= { id-mod 5 }
id-mod-ers-scvp-v1  OBJECT IDENTIFIER ::= { id-mod 5 1 }
```

The Data Structure for the Security Suitability of Cryptographic Algorithms (DSSC) [RFC5698] includes two ASN.1 modules. Both modules define the same syntax, but one module uses the 1997 ASN.1 syntax, and the other module uses the 1988 ASN.1 syntax. These module identifiers are:

```
id-mod-dssc88       OBJECT IDENTIFIER ::= { id-mod 6 }
id-mod-dssc88-v1    OBJECT IDENTIFIER ::= { id-mod 6 1 }
id-mod-dssc         OBJECT IDENTIFIER ::= { id-mod 7 }
id-mod-dssc-v1      OBJECT IDENTIFIER ::= { id-mod 7 1 }
```

4. CMS Content Types

A CMS content type for an Evidence Record was reserved, but no specification points to this value. It remains reserved.

```
id-ct-evidence-record  OBJECT IDENTIFIER ::= { id-ct 1 }
```

The Data Structure for the Security Suitability of Cryptographic Algorithms (DSSC) [RFC5698] specifies three CMS content types. These CMS content types are:

```
id-ct-dssc-asn1        OBJECT IDENTIFIER ::= { id-ct 2 }
id-ct-dssc-xml         OBJECT IDENTIFIER ::= { id-ct 3 }
id-ct-dssc-tbsPolicy   OBJECT IDENTIFIER ::= { id-ct 6 }
```

The Long-term Archive Protocol (LTAP) [LTAP] defines two CMS content types. While this protocol was never published as an RFC, the CMS content types were assigned to facilitate implementation. These CMS content types are:

```
id-ct-LTAPRequest      OBJECT IDENTIFIER ::= { id-ct 4 }
id-ct-LTAPResponse     OBJECT IDENTIFIER ::= { id-ct 5 }
```

5. ERS Encryption Methods

An arc was set up for Evidence Record Syntax (ERS) encryption methods, and one object identifier was assigned. However, that object identifier is obsolete, and it should not be used.

```
id-em-enveloped-data OBJECT IDENTIFIER ::= { id-em 1 } -- obsolete
```

6. Security Considerations

This document populates an IANA registry, and it raises no new security considerations. The protocols that specify these values include the security considerations associated with their usage.

7. IANA Considerations

IANA has updated one registry table and created four additional tables.

Updates to the four new tables require Expert Review, as defined in [RFC5226]. The Designated Expert is expected to ensure that any new values are strongly related to the work that was done by the LTANS WG. Object identifiers for other purposes should not be assigned in this arc.

7.1. SMI Security for Mechanism Codes Registry

The reference in the Long-Term Archive and Notary Services entry (decimal value 11) has been updated so that it points to this document.

7.2. SMI Security for LTANS Registry

Within the SMI Security Codes registry, IANA has added an "SMI Security for LTANS (1.3.6.1.5.5.11)" table with three columns:

Decimal	Description	References
0	module-identifiers	[RFC7036]
1	cms-content-types	[RFC7036]
2	ers-encryption-methods	[RFC7036]

Future updates to this table require Expert Review, as defined in [RFC5226].

7.3. SMI Security for LTANS Module Identifier Registry

Within the SMI Security Codes registry, IANA has added an "SMI Security for LTANS Module Identifier (1.3.6.1.5.5.11.0)" table with three columns:

OID Value	Description	References
1.3.6.1.5.5.11.0.1	id-mod-ers	[RFC4998]
1.3.6.1.5.5.11.0.1.1	id-mod-ers-v1	[RFC4998]
1.3.6.1.5.5.11.0.2	id-mod-ers88	[RFC4998]
1.3.6.1.5.5.11.0.2.1	id-mod-ers88-v1	[RFC4998]
1.3.6.1.5.5.11.0.3	id-mod-ltap88	Reserved
1.3.6.1.5.5.11.0.3.0	id-mod-ltap88-v0	Reserved
1.3.6.1.5.5.11.0.3.1	id-mod-ltap88-v1	Reserved
1.3.6.1.5.5.11.0.4	id-mod-ltap	Reserved
1.3.6.1.5.5.11.0.4.0	id-mod-ltap-v0	Reserved
1.3.6.1.5.5.11.0.4.1	id-mod-ltap-v1	Reserved
1.3.6.1.5.5.11.0.5	id-mod-ers-scvp	[RFC5276]
1.3.6.1.5.5.11.0.5.1	id-mod-ers-scvp-v1	[RFC5276]
1.3.6.1.5.5.11.0.6	id-mod-dssc88	[RFC5698]
1.3.6.1.5.5.11.0.6.1	id-mod-dssc88-v1	[RFC5698]
1.3.6.1.5.5.11.0.7	id-mod-dssc	[RFC5698]
1.3.6.1.5.5.11.0.7.1	id-mod-dssc-v1	[RFC5698]

Future updates to this table require Expert Review, as defined in [RFC5226].

7.4. SMI Security for LTANS CMS Content Type Registry

Within the SMI Security Codes registry, IANA has added an "SMI Security for LTANS CMS Content Type (1.3.6.1.5.5.11.1)" table with three columns:

Decimal	Description	References
1	id-ct-evidence-record	Reserved
2	id-ct-dssc-asn1	[RFC5698]
3	id-ct-dssc-xml	[RFC5698]
4	id-ct-LTAPRequest	Reserved
5	id-ct-LTAPResponse	Reserved
6	id-ct-dssc-tbsPolicy	[RFC5698]

Future updates to this table require Expert Review, as defined in [RFC5226].

7.5. SMI Security for LTANS ERS Encryption Method Registry

Within the SMI Security Codes registry, add an "SMI Security for LTANS ERS Encryption Method (1.3.6.1.5.5.11.2)" table with three columns:

Decimal	Description	References
1	id-em-enveloped-data	Reserved and Obsolete

Future updates to this table require Expert Review, as defined in [RFC5226].

8. References

8.1. Normative References

[ASN1-88] International Telephone and Telegraph Consultative Committee, "Specification of Abstract Syntax Notation One (ASN.1)", CCITT Recommendation X.208, 1988.

[ASN1-97] International Telecommunications Union, "Abstract Syntax Notation One (ASN.1): Specification of basic notation", ITU-T Recommendation X.680, 1997.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

8.2. Informative References

[LTAP] Jerman Blazic, A., Sylvester, P., and C. Wallace, "Long-term Archive Protocol (LTAP)", Work in Progress, July 2009.

[RFC4998] Gondrom, T., Brandner, R., and U. Pordesch, "Evidence Record Syntax (ERS)", RFC 4998, August 2007.

[RFC5276] Wallace, C., "Using the Server-Based Certificate Validation Protocol (SCVP) to Convey Long-Term Evidence Records", RFC 5276, August 2008.

[RFC5698] Kunz, T., Okunick, S., and U. Pordesch, "Data Structure for the Security Suitability of Cryptographic Algorithms (DSSC)", RFC 5698, November 2009.

9. Acknowledgements

Thanks to Carl Wallace, Sean Turner, Paul Hoffman, and Carsten Bormann for their review and comments.

Author’s Address

Russ Housley
Vigil Security, LLC
918 Spring Knoll Drive
Herndon, VA 20170
USA

EMail: housley@vigilsec.com