Internet Engineering Task Force (IETF)
Internet Draft
Intended Status: Informational
Expires: November 22, 2013

S. Turner
IECA
R. Housley
Vigil Security
J. Schaad
Soaring Hawk Consulting

May 21, 2013

The application/cms media type
draft-turner-application-cms-media-type-01.txt

Abstract

This document registers the application/cms media types for use with the corresponding CMS (Cryptographic Message Syntax) content types.

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 http://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."

1. Introduction

[RFC5751] registered the application/pkc7-mime media type. That document defined five optional smime-type parameters. The smime-type parameter originally conveyed details about the security applied (signed or enveloped) to the data content type, hence signed-data and enveloped-data, the name of the data, and was later expanded to also indicate that the message was compressed, compressed-data, and that the message is a certs-only message. This document does not affect those registrations as this document places no requirements on S/MIME (Secure Multipurpose Internet Mail Extensions) agents.

The registration done by the S/MIME documents was done assuming that there would be a MIME (Multipurpose Internet Mail Extensions) wrapping layer around each of the different enveloping contents, thus there was no need to include more than one item in each smime-type. This is no longer the case with some of the more advanced enveloping types. Some protocols such as the CMC (Certificate Management over Cryptographic Message Syntax) [CMC] have defined additional S/MIME types. New protocols that intend to wrap MIME content should continue to define an smime-type string, however new protocols that intend to wrap non-mime types should use this mechanism instead.

CMS (Cryptographic Message Syntax) [RFC5652] associates a content type identifier (OID) with a content; CMS content types have been widely used to define contents that can be enveloped using other CMS content types and to define enveloping content types some of which provide security services. CMS protecting content types, those that provide security services, include: id-signedData [RFC5652], id-envelopedData [RFC5652], id-digestData [RFC5652], id-encryptedData [RFC5652], id-ct-authData [RFC5652], id-ct-authEnvelopedData [RFC5083], and id-ct-KP-encryptedKeyPkg [RFC6032]. CMS non-protecting content types, those that provide no security services but encapsulate other CMS content types, include: id-ct-contentInfo [RFC5652], id-compressedData [RFC3274], id-ct-contentCollection [RFC4073], and id-ct-contentWithAttrs [RFC4073]. Then, there are the inner most content types that include: id-data [RFC5652], id-ct-KP-aKeyPackage [RFC5958], id-ct-KP-sKeyPackage [RFC6031], id-ct-firmwarePackage [RFC4108], id-ct-firmwareLoadReceipt [RFC4108], id-ct-firmwareLoadError [RFC4108], id-ct-trustAnchorList [RFC5914], id-ct-KP-keyPackageReceipt [ID.housley-keypackage-receipt-n-error], and id-ct-KP-keyPackageError [ID.housley-keypackage-receipt-n-error].

To support conveying CMS content types, this document defines a media type and parameters that indicate the enveloping and embedded CMS content types.

Note that this document uses the ASN.1 label for the object

identifier in identifying new OID types. This trend is expected to continue. However new CMS content types should be affirmative in defining the string that identifies the new content type and should additionally define if the new content type is expected to appear in the encapsulatedContent or innerContent field.

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. CMS Media Type Registration Applications

This section provides the media type registration application for the application/cms media type (see [RFC6838], Section 5.6).

Type name: application

Subtype name: cms

Required parameters: None.

Optional parameters:

encapsulatedContent=y; where y is one or more CMS ECT (Encapsulating Content Types); multiple values are separated by a folding-whitespace comma folding-whitespace. If folding-whitespace is used then the set of values must be quoted. Currently defined CMS ECTs OID names are found in [RFC3274], [RFC4073], [RFC5083], [RFC5652], and [RFC6032]:

```
id-authData
id-compressedData
id-ct-contentCollection
id-ct-contentInfo
id-ct-contentWithAttrs
id-ct-authEnvelopedData
id-ct-KP-encryptedKeyPkg
id-digestData
id-encryptedData
id-envelopedData
id-signedData
```

The values for y can be any content type that encapsulates another content type.

innerContent=x; where x is one or more CMS ICT (Inner Content Types); multiple values are separated by a folding-whitespace comma

folding-whitespace. If folding-whitespace is used then the set of values must be quoted.

ict=id-ct-KP-aKeyPackage, id-ct-KP-sKeyPackage). The following are ICTs defined in [RFC4108], [RFC5652], [RFC5914], [RFC5958], [RFC6031], and [ID.housley-keypackage-receipt-n-error]:

id-ct-firmwarePackage
id-ct-firmwareLoadReceipt
id-ct-firmwareLoadError
id-ct-KP-aKeyPackage
id-ct-KP-sKeyPackage
id-ct-trustAnchorList
id-ct-KP-keyPackageReceipt
id-ct-KP-keyPackageError

The values for x can be any content type that does not encapsulate another content type. id-data MUST NOT be used; id-data encapsulation uses the application/pkcs7-mime media type defined in [RFC5751].

The optional parameters are case-sensitive.

Encoding considerations:

Binary.

[RFC5652] requires that the outer most encapsulation be ContentInfo.

Security considerations:

See [RFC5652], [RFC3370], [RFC5753], and [RFC5754] for id-signedData, id-envelopedData, id-digestData, id-encryptedData, id-ct-authData; see [RFC5958], [RFC5959], and [RFC6162] for id-ct-KP-aKeyPackage; see [RFC6031] and [RFC6160] for id-ct-KP- sKeyPackage; see [RFC6032], [RFC6033], and [RFC6161] for id-ct-KP-encryptedKeyPkg; see [RFC5914] for id-ct-trustAnchorList; see [RFC3274] for id-compressedData; see [RFC5083] and [RFC5084] for id-ct-authEnvelopedData; see [RFC4073] for id-ct-contentCollection and id-ct-contentWithAttrs; see [RFC4108] for id-ct-firmwarePackage, id-ct-firmwareLoadReceipt, id-ct-firmwareLoadError; see [ID.housley-keypackage-receipt-n-error] for id-ct-KP-keyPackageReceipt and id-ct-KP-keyPackageError.

Interoperability considerations:

See [RFC3274], [RFC4073], [RFC4108], [RFC5083], [RFC5652], [RFC5958], [RFC5914], [RFC6031], [RFC6032], and [ID.housley-

keypackage-receipt-n-error].

In all cases, CMS content types are encapsulated within ContentInfo structures [RFC5652]; that is the outer most enveloping structure is ContentInfo.

When processing a SignedData around any of the inner content type the [RFC5652] validation rules MUST be used. The PKCS #7 [RFC2315] validation rules MUST NOT be used.

Published specification: This specification.

Applications which use this media type:

Applications that support CMS (Cryptographic Message Syntax) content types.

Additional information:

Magic number(s): None
File extension(s): .cms
Macintosh File Type Code(s):

Person & email address to contact for further information:

Sean Turner <turners@ieca.com>

Restrictions on usage: none

Author: Sean Turner <turners@ieca.com>

Intended usage: COMMON

Change controller: The IESG <iesg@ietf.org>

3. IANA Considerations

IANA is asked to register the media type application/cms in the Standards tree using the applications provided in Section 2 of this document.

4. Security Considerations

No new security considerations are introduced in additional those specified in [RFC3274], [RFC3370], [RFC4073], [RFC4108], [RFC5083], [RFC5084], [RFC5652], [RFC5753], [RFC5754], [RFC5914], [RFC5958], [RFC6031], [RFC6032], [RFC6033], [RFC6160], [RFC6161], [RFC6162], and

[ID.housley-keypackage-receipt-n-error].

5. References

5.1. Normative References

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

[RFC3274] Gutmann, P., "Compressed Data Content Type for Cryptographic Message Syntax (CMS)", RFC 3274, June 2002.

[RFC3370] Housley, R., "Cryptographic Message Syntax (CMS) Algorithms", RFC 3370, August 2002.

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

[RFC4108] Housley, R., "Using Cryptographic Message Syntax (CMS) to Protect Firmware Packages", RFC 4108, August 2005.

[RFC5083] Housley, R., "Cryptographic Message Syntax (CMS) Authenticated-Enveloped-Data Content Type", RFC 5083, November 2007.

[RFC5084] Housley, R., "Using AES-CCM and AES-GCM Authenticated Encryption in the Cryptographic Message Syntax (CMS)", RFC 5084, November 2007.

[RFC5652] Housley, R., "Cryptographic Message Syntax (CMS)", STD 70, RFC 5652, September 2009.

[RFC5753] Turner, S. and D. Brown, "Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS)", RFC 5753, January 2010.

[RFC5754] Turner, S., "Using SHA2 Algorithms with Cryptographic Message Syntax", RFC 5754, January 2010.

[RFC5914] Housley, R., Ashmore, S., and C. Wallace, "Trust Anchor Format", RFC 5914, June 2010.

[RFC5958] Turner, S., "Asymmetric Key Packages", RFC 5958, August 2010.

[RFC5959] Turner, S., "Algorithms for Asymmetric Key Package Content Type", RFC 5959, August 2010.

[RFC6031] Turner, S. and R. Housley, "Cryptographic Message Syntax (CMS) Symmetric Key Package Content Type", RFC 6031, December 2010.

[RFC6032] Turner, S. and R. Housley, "Cryptographic Message Syntax (CMS) Encrypted Key Package Content Type", RFC 6032, December 2010.

[RFC6033] Turner, S., "Algorithms for Cryptographic Message Syntax (CMS) Encrypted Key Package Content Type", RFC 6033, December 2010.

[RFC6160] Turner, S., "Algorithms for Cryptographic Message Syntax (CMS) Protection of Symmetric Key Package Content Types", RFC 6160, April 2011.

[RFC6838] Freed, N., Klensin, J., and T. Hansen, "Media Type Specifications and Registration Procedures", BCP 13, RFC 6838, January 2013.

[ID.housley-keypackage-receipt-n-error] Housley, R., "Cryptographic Message Syntax (CMS) Key Package Receipt and Error Content Types", draft-housley-ct-keypackage-receipt-n-error, May 2013.

5.2. Informative References

[RFC2315] Kaliski, B., "PKCS #7: Cryptographic Message Syntax Version 1.5", RFC 2315, March 1998.

[RFC5751] Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification", RFC 5751, January 2010.

Authors' Addresses

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

EMail: turners@ieca.com
Phone: +1.703.628.3180

Russell Housley
Vigil Security, LLC
918 Spring Knoll Drive

Herndon, VA 20170
USA

EMail: housley@vigilsec.com

Jim Schaad
Soaring Hawk Consulting

EMail: jimsch@augustcellars.com