                      The application/cms Media Type

Abstract

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

Status of This Memo

Copyright Notice

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 to
   the data content type, indicating whether it was signed or enveloped,
   as well as the name of the data content; it was later expanded to
   indicate whether the data content is compressed and whether the data
   content contained 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) [RFC5273] have defined
   additional S/MIME types. New protocols that intend to wrap MIME
   content should continue to define a 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 specific 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: Signed-Data [RFC5652],
   Enveloped-Data [RFC5652], Digested-Data [RFC5652], Encrypted-Data
   [RFC5652], Authenticated-Data [RFC5652], Authenticated-Enveloped-Data
   [RFC5083], and Encrypted Key Package [RFC6032]. CMS non-protecting
   content types, those that provide no security services but
   encapsulate other CMS content types, include: Content Information
   [RFC5652], Compressed Data [RFC3274], Content Collection [RFC4073],
   and Content With Attributes [RFC4073]. Then, there are the innermost
   content types that include: Data [RFC5652], Asymmetric Key Package
   [RFC5958], Symmetric Key Package [RFC6031], Firmware Package
   [RFC4108], Firmware Package Load Receipt [RFC4108], Firmware Package
   Load Error [RFC4108], Trust Anchor List [RFC5914], TAMP Status Query,
   TAMP Status Response, TAMP Update, TAMP Update Confirm, TAMP Apex
   Update, TAMP Apex Update Confirmation, TAMP Community Update, TAMP
   Community Update Confirm, TAMP Sequence Adjust, TAMP Sequence Adjust
   Confirmation, TAMP Error [RFC5934], Key Package Error, and Key
   Package Receipt [RFC7191].

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

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 parameter.

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:

encapsulatingContent=y; where y is one or more CMS ECT
(Encapsulating Content Type) identifiers; multiple values are
encapsulated in quotes and separated by a folding-whitespace, a
comma, and folding-whitespace. ECT values are based on content
types found in [RFC3274], [RFC4073], [RFC5083], [RFC5652], and
[RFC6032]. This list can later be extended; see Section 4.

    authData
    compressedData
    contentCollection
    contentInfo
    contentWithAttrs
    authEnvelopedData
    encryptedKeyPkg
    digestData
    encryptedData
    envelopedData
    signedData

   innerContent=x; where x is one or more CMS ICT (Inner Content Type)
   identifiers; multiple values encapsulated in quotes and are separated
   by a folding-whitespace, a comma, and folding-whitespace. ICT values
   are based on content types found in [RFC4108], [RFC5914], [RFC5934],
   [RFC5958], [RFC6031], and [RFC7191]. This list can later be
   extended; see Section 4.

        firmwarePackage
        firmwareLoadReceipt
        firmwareLoadError
        aKeyPackage
        sKeyPackage
        trustAnchorList
        TAMP-statusQuery
        TAMP-statusResponse
        TAMP-update
        TAMP-updateConfirm
        TAMP-apexUpdate
        TAMP-apexUpdateConfirm
        TAMP-communityUpdate
        TAMP-communityUpdateConfirm
        TAMP-seqNumAdjust
        TAMP-seqNumAdjustConfirm
        TAMP-error
        keyPackageReceipt
        keyPackageError

   The optional parameters are case sensitive.

   Encoding considerations:

      Binary.

      [RFC5652] requires that the outermost encapsulation be
      ContentInfo.

Security considerations:

The following security considerations apply:

```
RFC       | CMS Protecting Content Type and Algorithms
----------+-------------------------------------------
[RFC3370] | signedData, envelopedData,
[RFC5652] | digestedData, encryptedData, and
[RFC5753] | authData
[RFC5754] |
----------+-------------------------------------------
[RFC5958] | aKeyPackage
[RFC5959] |
[RFC6162] |
----------+-------------------------------------------
[RFC6031] | sKeyPackage
[RFC6160] |
----------+-------------------------------------------
[RFC6032] | encryptedKeyPkg
[RFC6033] |
[RFC6161] |
----------+-------------------------------------------
[RFC5914] | trustAnchorList
----------+-------------------------------------------
[RFC3274] | compressedData
----------+-------------------------------------------
[RFC5083] | authEnvelopedData
[RFC5084] |
----------+-------------------------------------------
[RFC4073] | contentCollection and
          | contentWithAttrs
----------+-------------------------------------------
[RFC4108] | firmwarePackage,
          | firmwareLoadReceipt, and
          | firmwareLoadError
----------+-------------------------------------------
[RFC5934] | TAMP-statusQuery, TAMP-statusResponse,
          | TAMP-update, TAMP-updateConfirm,
          | TAMP-apexUpdate,
          | TAMP-apexUpdateConfirm,
          | TAMP-communityUpdate,
          | TAMP-communityUpdateConfirm,
          | TAMP-seqNumAdjust,
          | TAMP-seqNumAdjustConfirm, and
          | TAMP-error
----------+-------------------------------------------
[RFC7191] |keyPackageReceipt and keyPackageError
----------+-------------------------------------------
```

In some circumstances, significant information can be leaked by disclosing what the innermost ASN.1 structure is. In these cases, it is acceptable to disclose the wrappers without disclosing the inner content type.

ASN.1 encoding rules (e.g., DER and BER) have a type-length-value structure, and it is easy to construct malicious content with invalid length fields that can cause buffer overrun conditions. ASN.1 encoding rules allows for arbitrary levels of nesting, which may make it possible to construct malicious content that will cause a stack overflow. Interpreters of ASN.1 structures should be aware of these issues and should take appropriate measures to guard against buffer overflows and stack overruns in particular and malicious content in general.

Interoperability considerations:

See [RFC3274], [RFC4073], [RFC4108], [RFC5083], [RFC5652], [RFC5914], [RFC5934], [RFC5958], [RFC6031], [RFC6032], and [RFC7191].

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

CMS [RFC5652] defines slightly different processing rules for SignedData than does PKCS #7 [RFC2315]. This media type employs the CMS processing rules.

The Content-Type header field of all application/cms objects SHOULD include the optional "encapsulatingContent" and "innerContent" parameters.

The Content-Disposition header field [RFC4021] can also be included along with Content-Type's optional name parameter.

Published specification: This specification.

Applications that use this media type:

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

Fragment identifier considerations: N/A

Additional information:

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

Person & email address to contact for further information:

Sean Turner <turners@ieca.com>

Intended usage: COMMON

Restrictions on usage: none

Author: Sean Turner <turners@ieca.com>

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

3. Example

    The following is an example encrypted status response message:

        MIME-Version: 1.0
        Content-Type: application/cms; encapsulatingContent=encryptedData;
                    innerContent=TAMP-statusResponse; name=status.cmsc
        Content-Transfer-Encoding: base64

        MIIFLQYJKoZIhvcNAQcDoIIFHjCCBRoCAQAxggFhMIIBXQIBADBFMEAxC
        zAJBgNVBAYTAlVTMR8wHQYDVQQKExZUZXN0IENlcnRpZmljYXRlcyAyMD
        ExMRAwDgYDVQQDEwdHb29kIENBMAgEBMA0GCSqGSIb3DQEBAQUABIIBAEa
        uaXQeVsOyZ7gz0pJikRQ6Jqr64k2dbHBE4SDZL/uErP9FJUIja9LaJrc5
        S83EZ7wf3mODUBaDhGfQVKoPrNTsLmw98fE/O+wcdpI2XKaILOR62xDJR
        emQQST+EPfMwZmCwgsImmY3AxefAgzp8hVgK7SDiXGXfa9ux9PMdCSjHP
        IgcAUFHmTiqxYd72Gl08kLCMIXmn3g5RsYUggxooeFNHiFNR28TV5HctG
        i6Ay5++iKUGrUQyXD+GlwakFToGFmFj3FMyZi7+kYV/X00BiBP3kpIgVJ
        4jCj+nYtKWh6JXPoEqEsa39GmDEFGq4/58GEu70amWvW1DA++7kDP4gwg
        gOuBgkqhkiG9w0BBwEwHQYJYIZIAWUDBAECBBCH5yTQqZ4KYiTTeYdjoY
        4sgIIDgArSpOcengKnZS4SCjfuQkMxB5wfSaud1thlZ+gUFCgzbFtkfYM
        Qx/T7gnkneniyj2rwOmZxCQXpPlCDXH6mS83ngfrNN8ay3HrMPpVkEOmW
        UMc5jI6oNObwqi8a3ezzhYRxF06jzdD2R/6SAPALz3Q4NU8eX+PnuekgR
        oxo/INzhT4iGvokn9xVah6piSbjhPA+QZpIHgQrlWyyM3lG9jn4thchKl
        FQqZEy/EBaCWq+sJG7LLxqsS5k29CiAVx0JSItqAPvX1ZvLMY2aq//MQMw
        0VFEx7Kt5aWNvKHTor9RUuuzwiZ5kwXt2vJt6bFiV7yS+EXofpFEmqyJP
        VJzyAFIXJRTv4k007n0M1UpXQpGjywECI6DbIhfBL8CsNskTCjrsfU+Tw
        RRkRKAbtJYughs9bDYkDu9UsKd/AE4zXk4prwo8/f1chpmzpHKOXiWzt+
        xaCj648I4rOjdI9s4JP8J0qwVKoLEMGeiZlf2UlaiyMzZYzTOxI03PHp1
        Whk6TXhnmMVPWGYjjelvE38gq/XynobbQRGEJdnnHzH7SrS27FmgRcnBO
        3QQUPJChVn7iBHmdui++GAxpHoGdS6nSo4kQ6d5u5rL/Ctcnwu0k+s0Xi
        ZMzOqp7L31xl1jvYUWIswLQYsIFoiejU3UTKzq/Cpd5MK+I8cwCM3aQ2c
        D08URTPgu+U92pnYqm3auptywyjGAU/hkZ13XN7YRhLk/kuX8QXo3tZdj
        dKA4f/uNf1DURpJK9004uCkxuAtu5HemMv7YPTTx9Ua2pZFW5O+k2Mf2Z
        F/geOvtNw7UV8wOT1nokXu9lnIZ9Xcs1cGGmRYE7jW15F07uGnMi1s2Gt
        LAST7t/PlTNZU6h0rVExErVa7T+VNidrgwGIke0YqYIwvTINRs+9VeJE3
        AJeatDlQs+01jrqqFWWmGmmsEBTTRuoDQHK7YBFFy4xIwQqZGW0EVre39
        OU5CL5LHIYiAVoV16YwiGd5WvFF8P1ZJK4ki8GFgYiMcPKmjQgP7DumqG
        n7eQtMD5tezTQeC07ntV3bi5pdznZHVcF2Kqg+qHjJQlhUdK7Pew3kq7k
        mfCdQV0BmQSYyjEAaTijaw4fAMxAbiw4OU0eNeU//zcpp04AuTFfJorIg
        oZ+iCTYei8HMUA9/ysLFXA64wdsuCj0zXmNiYwosisuNg3TXfoBOzohKq
        fkeXt

4. IANA Considerations

    IANA has registered the media type application/cms in the Standards
    tree using the applications provided in Section 2 of this document.

IANA has established two subtype registries called "CMS Encapsulating
Content Types" and "CMS Inner Content Types". Entries in these
registries are allocated by Expert Review [RFC5226]. The Expert will
determine whether the content is an ECT or an ICT, where the rule is
that an ICT does not encapsulate another content type while an ECT
does encapsulate another content type.

Initial values are as follows:

CMS Encapsulating Content Types

```
Name                        | Document | Object Identifier
----------------------------+----------+--------------------------
authData                    |[RFC5652] | 1.2.840.113549.1.9.16.1.2
compressedData              |[RFC3274] | 1.2.840.113549.1.9.16.1.9
contentCollection           |[RFC4073] | 1.2.840.113549.1.9.16.1.19
contentInfo                 |[RFC5652] | 1.2.840.113549.1.9.16.1.6
contentWithAttrs            |[RFC4073] | 1.2.840.113549.1.9.16.1.20
authEnvelopedData           |[RFC5083] | 1.2.840.113549.1.9.16.1.23
encryptedKeyPkg             |[RFC6032] | 2.16.840.1.101.2.1.2.78.2
digestData                  |[RFC5652] | 1.2.840.113549.1.9.16.1.5
encryptedData               |[RFC5652] | 1.2.840.113549.1.9.16.1.6
envelopedData               |[RFC5652] | 1.2.840.113549.1.9.16.1.3
signedData                  |[RFC5652] | 1.2.840.113549.1.9.16.1.2
```

CMS Inner Content Types

```
Name                        | Document | Object Identifier
----------------------------+----------+--------------------------
firmwarePackage             |[RFC4108] | 1.2.840.113549.1.9.16.1.16
firmwareLoadReceipt         |[RFC4108] | 1.2.840.113549.1.9.16.1.17
firmwareLoadError           |[RFC4108] | 1.2.840.113549.1.9.16.1.18
aKeyPackage                 |[RFC5958] | 2.16.840.1.101.2.1.2.78.5
sKeyPackage                 |[RFC6031] | 1.2.840.113549.1.9.16.1.25
trustAnchorList             |[RFC5914] | 1.2.840.113549.1.9.16.1.34
TAMP-statusQuery            |[RFC5934] | 2.16.840.1.101.2.1.2.77.1
TAMP-statusResponse         |[RFC5934] | 2.16.840.1.101.2.1.2.77.2
TAMP-update                 |[RFC5934] | 2.16.840.1.101.2.1.2.77.3
TAMP-updateConfirm          |[RFC5934] | 2.16.840.1.101.2.1.2.77.4
TAMP-apexUpdate             |[RFC5934] | 2.16.840.1.101.2.1.2.77.5
TAMP-apexUpdateConfirm      |[RFC5934] | 2.16.840.1.101.2.1.2.77.6
TAMP-communityUpdate        |[RFC5934] | 2.16.840.1.101.2.1.2.77.7
TAMP-communityUpdateConfirm |[RFC5934] | 2.16.840.1.101.2.1.2.77.8
TAMP-seqNumAdjust           |[RFC5934] | 2.16.840.1.101.2.1.2.77.10
TAMP-seqNumAdjustConfirm    |[RFC5934] | 2.16.840.1.101.2.1.2.77.11
TAMP-error                  |[RFC5934] | 2.16.840.1.101.2.1.2.77.9
keyPackageReceipt           |[RFC7191] | 2.16.840.1.101.2.1.2.78.3
keyPackageError             |[RFC7191] | 2.16.840.1.101.2.1.2.78.6
```

5. Security Considerations

   See the answer to the Security Considerations template questions in
   Section 2.

6. Acknowledgments

   Special thanks to Carl Wallace for generating the example in
   Section 3.

7. References

7.1. 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.

   [RFC4021]   Klyne, G. and J. Palme, "Registration of Mail and MIME
               Header Fields", RFC 4021, March 2005.

   [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.

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

   [RFC5273]   Schaad, J. and M. Myers, "Certificate Management over CMS
               (CMC): Transport Protocols", RFC 5273, June 2008.

   [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.

   [RFC5934] Housley, R., Ashmore, S., and C. Wallace, "Trust Anchor
              Management Protocol (TAMP)", RFC 5934, August 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.

   [RFC6161] Turner, S., "Elliptic Curve Algorithms for Cryptographic
              Message Syntax (CMS) Encrypted Key Package Content Type",
              RFC 6161, April 2011.

   [RFC6162] Turner, S., "Elliptic Curve Algorithms for Cryptographic
              Message Syntax (CMS) Asymmetric Key Package Content Type",
              RFC 6162, April 2011.

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

   [RFC7191] Housley, R., "Cryptographic Message Syntax (CMS) Key
              Package Receipt and Error Content Types", RFC 7191, April
              2014.

7.2. 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: ietf@augustcellars.com