Network Working Group
Request for Comments: 3855
Category: Standards Track

P. Hoffman
IMC
C. Bonatti
IECA

July 2004

Transporting Secure/Multipurpose Internet Mail Extensions (S/MIME) Objects in X.400

Status of this Memo

Copyright Notice

Abstract

This document describes protocol options for conveying objects that have been protected using the Cryptographic Message Syntax (CMS) and Secure/Multipurpose Internet Mail Extensions (S/MIME) version 3.1 over an X.400 message transfer system.

1. Introduction

The techniques described in the Cryptographic Message Syntax [CMS] specification and message specifications can reasonably be transported via a variety of electronic mail systems. This specification defines the options and values necessary to enable interoperable transport of S/MIME messages over an X.400 system.

This document describes a mechanism for using CMS objects as the message content of X.400 messages in a native X.400 environment. This means that gateways or other functions that expect to deal with IPMS, such as those specified in [MIXER] and [BODYMAP], cannot do anything with these messages. Note that cooperating S/MIME agents must support common forms of message content in order to achieve interoperability.

Definition of gateway services to support relay of CMS object between X.400 and SMTP environments is beyond the scope of this document.

1.1. Terminology

The key words "MUST", "SHALL", "REQUIRED", "SHOULD", "RECOMMENDED", and "MAY" in this document are to be interpreted as described in BCP 14, RFC 2119 [MUSTSHOULD].

1.2. Definitions

For the purposes of this document, the following definitions apply.

ASN.1: Abstract Syntax Notation One, as defined in ISO/IEC 8824.

Object Identifier (OID): A globally unique identifier value consisting of a sequence of integer values assigned through distributed registration as specified by ISO/IEC 8824.

Transfer Encoding: A reversible transformation made on data so 8-bit or binary data may be sent via a channel that only transmits 7-bit data.

1.3. Compatibility with Existing S/MIME Implementations

It is a goal of this document to, if possible, maintain backward compatibility with existing X.400 implementations that employ S/MIME v3.1 wrappers.

2. S/MIME Packaging

2.1. The X.400 Message Structure

This section reviews the X.400 message format. An X.400 message has two parts, the envelope and the content, as described in X.402 [X.400]:

Envelope -- An information object whose composition varies from one transmittal step to another and that variously identifies the message's originator and potential recipients, documents its previous conveyance and directs its subsequent conveyance by the Message Transfer System (MTS), and characterizes its content.

Content -- The content is the piece of information that the originating User Agent wants to be delivered to one or more recipients. The MTS neither examines nor modifies the content, except for conversion, during its conveyance of the message. MTS conversion is not applicable to the scenario of this document because such conversion is incompatible with CMS protection mechanisms.

One piece of information borne by the envelope identifies the type of the content. The content type is an identifier (an ASN.1 OID or Integer) that denotes the syntax and semantics of the content overall. This identifier enables the MTS to determine the message's deliverability to particular users, and enables User Agents and Message Stores to interpret and process the content.

Some X.400 content types further refine the structure of content as a set of heading elements and body parts. An example of this is the Interpersonal Messaging System (IPMS). The IPMS content structure is able to convey zero or more arbitrary body parts each identified by the body part type. The body part type is an ASN.1 OID or Integer that denotes the syntax and semantics of the body part in question.

2.2. Carrying S/MIME as X.400 Content

When transporting a CMS-protected message in X.400, the preferred approach (except as discussed in section 2.3 below) is to convey the object as X.400 message content. This section describes how S/MIME CMS objects are conveyed as the content part of X.400 messages. This mechanism is suitable for transport of CMS-protected messages regardless of the mail content that has been encapsulated.

Implementations MUST include the CMS object in the content field of the X.400 message.

If the CMS object is covered by an outer MIME wrapper, the content-type field of the P1 envelope MUST be set to the following CMS-defined value:

```
id-data OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
      rsadsi(113549) pkcs(1) pkcs7(7) 1 }
```

If the CMS object is not covered by an outer MIME wrapper, the content-type field of the P1 envelope MUST be set to the following CMS-defined value:

```
id-ct-contentInfo  OBJECT IDENTIFIER ::= { iso(1) member-body(2)
      us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16)
      content-types(1) 6}
```

2.2.1. Carrying Plaintext MIME objects as X.400 Content

When transporting a plaintext MIME object in X.400, the preferred approach is to convey the object as X.400 message content. The

content-type field of the P1 envelope MUST be set to the following CMS-defined value:

```
id-data OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
      rsadsi(113549) pkcs(1) pkcs7(7) 1 }
```

2.3. Carrying S/MIME as IPMS Body Parts

Under some circumstances S/MIME CMS-protected messages can be conveyed within select body parts of the content. Implementations generally SHOULD NOT embed CMS objects within X.400 body parts, but should instead convey them as content as described in section 2.2. Nevertheless, one notable exception is necessary for the case of forwarding.

In instances when CMS objects are forwarded as part of a message forwarding function, use of a body part is necessary. When forwarding a CMS object in an IPMS or IPMS-compatible body part, implementations MUST use the content-body-part as formally defined by [X.400], as shown below for reference.

```
content-body-part {ExtendedContentType:content-type}
    EXTENDED-BODY-PART-TYPE ::= {
        PARAMETERS {ForwardedContentParameters IDENTIFIED BY
            {id-ep-content -- concatenated with content-type -- }},
        DATA {Content IDENTIFIED BY
            {id-et-content -- concatenated with content-type -- }} }

ForwardedContentParameters ::= SET {
    delivery-time     [0] MessageDeliveryTime OPTIONAL,
    delivery-envelope [1] OtherMessageDeliveryFields OPTIONAL,
    mts-identifier    [2] MessageDeliveryIdentifier OPTIONAL }

id-ep-content ::= {joint-iso-itu-t(2) mhs(6) ipms(1) ep(11) 17}

id-et-content ::= {joint-iso-itu-t(2) mhs(6) ipms(1) et(4) 17}
```

The implementation MUST copy the CMS object to be forwarded into the Content field of the content-body-part. The direct-reference field of the body part MUST include the OID formed by the concatenation of the id-et-content value and the following CMS-defined value.

```
id-ct-contentInfo  OBJECT IDENTIFIER ::=
      { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
      pkcs-9(9) smime(16) content-types(1) 6}
```

For example, to forward any CMS object the DATA component of the body part would be identified by { 2 6 1 4 17 1 2 840 113549 1 9 16 1 6 }.

The ForwardedContentParameters are optional and MAY be supported at the discretion of the implementor. The OID value id-et-content MAY also be included in the original-encoded-information-types field of the X.400 message envelope at the discretion of the sending S/MIME agent.

In this instance, the content-type field of the P1 envelope MUST be set to the value associate with the forwarding content (e.g., integer 22 for IPMS).

2.4. Transfer Encoding

According to various S/MIME specifications for message wrapping, CMS objects MAY optionally be wrapped in MIME to dynamically support 7-bit transport. This outer wrapping is not required for X.400 transport, and generally SHOULD NOT be applied in a homogeneous X.400 environment. Heterogeneous mail systems or other factors MAY require the presence of this outer MIME wrapper

2.5. Encoded Information Type Indication

In [MSG], the application/pkcs7-mime content type and optional "smime-type" parameter are used to convey details about the security applied (signed or enveloped) along with information about the contained content. This may aid receiving S/MIME implementations in correctly processing the secured content. Additional values of smime-type are defined in [ESS]. In an X.400 transport environment, MIME typing is not available. Therefore the equivalent semantic is conveyed using the Encoded Information Types (EITs). The EITs are conveyed in the original-encoded-information-types field of the X.400 message envelope. This memo defines the following smime-types.

smime-type CMS protection type	EIT Value (OID) Inner Content
enveloped-data EnvelopedData	id-eit-envelopedData Data
signed-data SignedData	id-eit-signedData Data
certs-only SignedData	id-eit-certsOnly empty (zero-length content)
signed-receipt SignedData	id-eit-signedReceipt Receipt
enveloped-x400 EnvelopedData	id-eit-envelopedx400 X.400 content
signed-x400 SignedData	id-eit-signedx400 X.400 content
compressed-data CompressedData	id-eit-compressedData RFC 3274 compression wrapper

Sending agents SHOULD include the appropriate S/MIME EIT OID value. Receiving agents SHOULD recognize S/MIME OID values in the EITs field, and process the message appropriately according to local procedures.

In order that consistency can be obtained in future S/MIME EIT assignments, the following guidelines should be followed when assigning new EIT values. Values assigned for S/MIME EITs should correspond to assigned smime-type values on a one-to-one basis. The restrictions of section 3.2.2 of [MSG] therefore apply. S/MIME EIT values may coexist with other EIT values intended to further qualify the makeup of the protected content.

2.5.1. Enveloped Data

The enveloped data EIT indicates that the X.400 content field contains a MIME type that has been protected by the CMS enveloped-data content type in accordance with [MSG]. The resulting enveloped data CMS content is conveyed in accordance with section 2.2. This EIT should be indicated by the following OID value:

```
id-eit-envelopedData  OBJECT IDENTIFIER ::=
    { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
    pkcs-9(9) smime(16) id-eit(10) id-eit-envelopedData(1) }
```

2.5.2. Signed Data

The signed data EIT indicates that the X.400 content field contains a MIME type that has been protected by the CMS signed-data content type in accordance with [MSG]. The resulting signed data CMS content is conveyed in accordance with section 2.2. This EIT should be indicated by the following OID value:

```
id-eit-signedData  OBJECT IDENTIFIER ::=
     { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
     pkcs-9(9) smime(16) id-eit(10) id-eit-signedData(2) }
```

2.5.3. Certs Only

The certs-only message is used to transport certificates and/or CRLs, such as in response to a registration request. This is described in [CERT31]. The certs-only message consists of a single instance of CMS content of type signed-data. The encapContentInfo eContent field MUST be absent and signerInfos field MUST be empty. The resulting certs-only CMS content is conveyed in accordance with section 2.2. This EIT should be indicated by the following OID value:

```
id-eit-certsOnly  OBJECT IDENTIFIER ::=
    { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
    pkcs-9(9) smime(16) id-eit(10) id-eit-certsOnly(3) }
```

2.5.4. Signed Receipt

The signed receipt EIT indicates that the X.400 content field contains a Receipt content that has been protected by the CMS signed-data content type in accordance with [ESS]. The resulting CMS signed-data content is conveyed in accordance with section 2.2. This EIT should be indicated by the following OID value:

```
id-eit-signedReceipt  OBJECT IDENTIFIER ::=
    { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
    pkcs-9(9) smime(16) id-eit(10) id-eit-signedReceipt(4) }
```

2.5.5. Enveloped X.400

The enveloped X.400 EIT indicates that the X.400 content field contains X.400 content that has been protected by the CMS enveloped-data content type in accordance with [X400WRAP]. The resulting enveloped X.400 CMS content is conveyed in accordance with section 2.2. This EIT should be indicated by the following OID value:

```
id-eit-envelopedX400  OBJECT IDENTIFIER ::=
    { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
    pkcs-9(9) smime(16) id-eit(10) id-eit-envelopedX400(5) }
```

2.5.6. Signed X.400

The signed X.400 EIT indicates that the X.400 content field contains X.400 content that has been protected by the CMS signed-data content type in accordance with [X400WRAP]. The resulting signed X.400 CMS content is conveyed in accordance with section 2.2. This EIT should be indicated by the following OID value:

```
id-eit-signedX400  OBJECT IDENTIFIER ::=
    { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
    pkcs-9(9) smime(16) id-eit(10) id-eit-signedX400(6) }
```

2.5.7. Compressed Data

The compressed data EIT indicates that the X.400 content field contains a another type that has been compressed by the compressed-data content type in accordance with [COMPRESS]. The resulting CMS content is conveyed in accordance with section 2.2. This EIT should be indicated by the following OID value:

```
id-eit-compressedData  OBJECT IDENTIFIER ::=
    { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
    pkcs-9(9) smime(16) id-eit(10) id-eit-compressedData(7) }
```

2.6. Interaction with X.400 Elements of Service

Care should be taken in the selection of X.400 services to be used in conjunction with CMS objects. Services affecting conversion of the content, expansion of Distribution Lists (DLs), and message redirection can interact badly with services provided by the "EnvelopedData" and "SignedData" CMS content types.

2.6.1. MTS Conversion Services

MTS conversion is not applicable to the scenario of this document because such conversion is incompatible with CMS protection mechanisms. X.400 systems that implement conversion services should generally be unable to attempt conversion of CMS content types because those types do not conform to X.420 structure rules. Nevertheless, when transporting CMS objects within an X.400 environment, the Conversion Prohibition service SHOULD be selected.

2.6.2. Message Redirection Services

X.400 message redirection services can have an indirect impact on the application of the CMS "EnvelopedData" content type. Several different forms of redirection are possible in X.400, including:

- Originator Requested Alternate Recipient (ORAR)
- Alternate Recipient Assignment
- Redirection of Incoming Messages

In addition, any auto-forwarding services that are not security-aware may share the same problem. An auto-forwarding implementation that removes the EnvelopedData and reapplies it for the forwarded recipient is not affected by this problem. The normal case is that the private key is not available when the human user is not present, thus decryption is not possible. However, if the private key is present, forwarding can be used instead.

When the "EnvelopedData" content type is used to protect message contents, an instance of RecipientInfo is needed for each recipient and alternate recipient in order to ensure the desired access to the message. A RecipientInfo for the originator is a good practice just in case the MTS returns the whole message.

In the event that ORAR is used, the originator is aware of the identity of the alternate recipient and SHOULD include a corresponding RecipientInfo element. For other forms of redirection (including non-security-aware auto-forwarding) the alternate recipient must either have access to the intended recipient’s keys (not recommended) or must relay the message to the intended recipient by other means.

2.6.3. DL Expansion

X.400 DLs can have an indirect impact on the application of the CMS "EnvelopedData" content type. When the "EnvelopedData" content type is used to protect message contents, an instance of RecipientInfo is needed for each recipient in order to ensure the desired access to

the message. Messages to a DL would typically include only a single RecipientInfo associated with the DL. Unlike Mail Lists (MLs) described in [ESS], however, X.400 DLs are not generally security-aware and do not regenerate RecipientInfo elements for the DL members. It is recommended that a security-aware ML conforming to [ESS] be used in preference to X.400 DLs. When transporting CMS objects within an X.400 environment, the DL Expansion Prohibited service SHOULD be selected.

3. Security Considerations

This specification introduces no new security concerns to the CMS or S/MIME models. Security issues are identified in section 5 of [MSG], section 6 of [ESS] and the Security Considerations section of [CMS].

4. References

4.1. Normative References

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

[CERT31] Ramsdell, B., Ed., "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Certificate Handling", RFC 3850, July 2004.

[CMS] Housley, R., "Cryptographic Message Syntax (CMS)", RFC 3852, July 2004.

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

[ESS] Hoffman, P., Ed., "Enhanced Security Services for S/MIME", RFC 2634, June 1999.

[MSG] Ramsdell, B., Ed., "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification", RFC 3851, July 2004.

[X.400] ITU-T X.400 Series of Recommendations, Information technology - Message Handling Systems (MHS). X.400: System and Service Overview; X.402: Overall Architecture; X.411: Message Transfer System: Abstract Service Definition and Procedures; X.420: Interpersonal Messaging System; 1996.

4.2. Informative References

[BODYMAP] Alvestrand, H., "Mapping between X.400 and RFC-822/MIME Message Bodies", RFC 2157, January 1998.

[MIXER] Kille, S., "MIXER (Mime Internet X.400 Enhanced Relay): Mapping between X.400 and RFC 822/MIME", RFC 2156, January 1998.

[X400WRAP] Hoffman, P., Bonatti, C., and A. Eggen, "Securing X.400 Content with Secure/Multipurpose Internet Mail Extensions (S/MIME), RFC 3854, July 2004.

5. Authors' Addresses

Paul Hoffman
Internet Mail Consortium
127 Segre Place
Santa Cruz, CA 95060 USA

EMail: phoffman@imc.org

Chris Bonatti
IECA, Inc.
15309 Turkey Foot Road
Darnestown, MD 20878-3640 USA

EMail: bonattic@ieca.com

6. Full Copyright Statement

Intellectual Property

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.