Network Working Group
Internet Draft
<draft-ietf-pem-mime-alternative-00.txt>

Internet Engineering Task Force
Privacy Enhanced Mail Working Group
J. I. Schiller
MIT

October 1993

An Alternative PEM MIME Integration

Status of this Memo

This is the second document to describe a mechanism to enclose MIME messages within PEM and vica versa. This document is an independent effort to be considered as an alternative to the previous document. This is *not* a revision of that document and the authors of it do not necessarily endorse the approach described here.

Introduction

This document describes a mechanism for providing Privacy Enhanced Mail (PEM) functionality within the context of MIME messages.

Background

MIME (RFC1341-1342) and PEM (RFC1421-1424) have taken separate evolution paths. Specifically PEM was designed and specified to handle RFC822 (non-MIME) messages. The goal of this document is to describe a method for using PEM to protect MIME messages, and to define a way to enclose PEM processed messages within MIME messages.

To accomplish these goals requires an additional profile for RFC1421 (Content-Domain: MIME) and the definition of a new MIME "application" (application/pem-1421).

There are four possibilities for interaction between PEM and MIME.

They are:

* A MIME message transporting an RFC1421 PEM message which itself contains an RFC822 message (Content-Domain: RFC822).

* A MIME message transporting an RFC1421 PEM message which itself contains a MIME object (Content-Domain: MIME).

Internet Engineering Task Force
Privacy Enhanced Mail Working Group
J. I. Schiller
MIT
October 1993

* A PEM message which contains a RFC822 message (as specified by RFC1421).

* A PEM message which contains a MIME message or object (Content-Domain: MIME).

Definition of "Content-Domain: MIME" within an RFC1421 PEM message

When a PEM message contains a MIME object, as opposed to a simple text message, the value of the Content-Domain field of the PEM headers shall be the string "MIME".

An RFC1421 PEM message of Content-Domain "MIME" shall contain a MIME "object" that begins with a "Content-Type" MIME header. The PEM body, upon completion of successful PEM processing is handed to a MIME interpreter for further processing. Content-Domain "MIME" messages may be protected with either ENCRYPTED, MIC-ONLY or MIC-CLEAR PEM services. However if MIC-CLEAR is chosen, the MIME content should be in a canonical 7bit form.

In other words, if the enclosed MIME object is encoded in such fashion as to be 7bit transportable, then MIC-CLEAR may be (and perhaps should be) used. Other non-encrypted messages should be encoded via the MIC-ONLY mechanism.

Enclosing a PEM message within a MIME object

An RFC1421 PEM message may be enclosed in a MIME message by defining it to be of Content Type "application/pem-1421" by preceding the PEM processed body with:

Content-Type: application/pem-1421

Note that the application subtype is defined to be "pem-1421" and that the representation *must* be text/plain; charset=us-ascii. This is because these are correct characterizations of what a RFC1421 message appears as.

The behavior of a MIME mail reader with PEM capability

A MIME mail reader with PEM capability will be able to fully process a MIME message which includes a PEM portion (which may either be the entire message or only part of a multi-part message).

The MIME reader will process a message which contains a PEM portion as it would any other MIME message. Upon encountering a

"application/pem-1421" body part, it will invoke PEM processing on the enclosed PEM message. If the PEM message contains a Content-Domain "MIME" body, it will invoke MIME recursively on the successfully processed PEM body. If the Content-Domain is RFC822, the PEM software will either display the enclosed text, or prepend the necessary headers such that it can be fed to a MIME reader which will treat it as an RFC822 mail message.

Internet Engineering Task Force
Privacy Enhanced Mail Working Group
J. I. Schiller
MIT
October 1993

The behavior of a MIME mail reader without PEM capability

A MIME mail reader will process a MIME message with PEM contents as any other MIME message. If an application/pem-1421 object is found and the MIME reader does not support PEM, then the MIME reader may handle the enclosed PEM message in the same or similar fashion as it handles any other application subtype for which it has no support software.

The behavior of a non-MIME but PEM capable mail reader

A PEM mail reader that does not understand MIME will be able to process a MIME/PEM message provided that the message itself is a PEM message. In other words, if the whole message is PEM processed as the last step prior to transmission, then a PEM capable, but non-MIME capable mail reader will be able to process the PEM message and then display the enclosed MIME object in the same fashion that a non-MIME mail reader handles a MIME (but non-PEM) message today.

It is likely that a non-MIME compliant mail reading agent may not be able to parse a MIME message in order to discover an enclosed "application/pem-1421" component containing a PEM message. However an end-user may be able to manually reformat the incoming message so as to make it amenable to PEM processing.

Discussion

Prior approaches to integrating PEM and MIME have suggested a significant departure from the RFC1421 PEM encapsulation mechanism. Specifically it has been recommended that PEM messages be represented as MIME multi-part messages. One part of the multi-part would contain what in RFC1421 is described as the PEM headers, and the other would contain the PEM body that is protected by the PEM mechanisms specified in the PEM header part.

This document intentionally does not recommend such an approach. This is because it is important for MIME interpreters to *not* reach down into the structure of a PEM body until PEM processing has been performed. The reason for this requirement has to do with the requirement that PEM body parts be immutable so that digital signatures computed on them can be verified. If a PEM body part is decomposeable by MIME readers, then it is quite possible that MIME gateways could reassemble PEM body parts in a fashion semantically equivalent to the original message, but sufficiently different (i.e., different in one bit is sufficient) to cause signature verification

to later fail.

It is important to understand that the signature verification requirement mandates that PEM messages be carried within MIME as "application" objects and not as "message", "multipart" or other types of body parts. Once this is recognized, it no longer matters whether or not the object within the "application" enclosure appears to be a MIME object upon visual inspection, for it is now outside the realm of what a MIME interpreter may attempt to parse without the aid of the application processor (PEM in this case).

Internet Engineering Task Force
Privacy Enhanced Mail Working Group
J. I. Schiller
MIT
October 1993

By using the RFC1421 based encapsulation technology we benefit from the experience gained in debugging existing PEM implementations as well as ease backward compatibility with non-MIME based PEM agents.

Examples

```
Date: Sun, 30 May 93 23:59:39 EST
From: jis@MIT.EDU (Jeffrey I. Schiller)
To: pem-dev@tis.com
Subject: Example PEM MIME Interaction
MIME-Version: 1.0
Content-Type: application/pem-1421

-----BEGIN PRIVACY-ENHANCED MESSAGE-----
Proc-Type: 4,MIC-CLEAR
Content-Domain: MIME
Originator-Certificate: MIIB+jCCAWMCAQIwDQYJKoZIhvcNAQECBQAwSj...
Issuer-Certificate: MIIB+jCCAWMCAQQwDQYJKoZIhvcNAQECBQAwRDELMA...
MIC-Info: RSA-MD5,RSA,dlSRMLFiwcK7FDvFef8gJfLWwMM4uxMSNtKGlLz9xxw
 fAyvaFuzp85davcwX4q7EImDs4K46Uwh0oL2GueLnv6b4s1gg25mMg/Y5Bd7/HaE
 cvkV77tKWGXZrDGEgGSDA

Content-Type: text/plain; charset=us-ascii

This is a test message.
-----END PRIVACY-ENHANCED MESSAGE-----
```

Author's Address

Jeffrey I. Schiller
Massachusetts Institute of Technology
MIT Room E40-311
1 Amherst Street
Cambridge, MA 02139
U.S.A.
Tel: +1 (617) 253-0161
Fax: +1 (617) 258-8736
Email: jis@mit.edu