

draft-ietf-lamps-header-protection

Daniel Kahn Gillmor

Bernie Hoeneisen

Alexey Melnikov

IETF 110 / LAMPS

lamps-header-protection-03

- Describes two schemes of header protection:
 - **Wrapped Message** (S/MIME 3.1+)
 - **Injected Headers** (draft-autocrypt, aka “memory hole”)
- How to compose them
 - For encrypted messages, **Header Confidentiality Policy**

lamps-header-protection-03 (administrivia)

- dkg picks up lead editor role from Bernie
- Document editing workflow now at
<https://gitlab.com/dkg/lamps-header-protection>

Two Header Protection Schemes

Only need to consider the Cryptographic Payload...

Wrapped Message

[...Cryptographic Envelope...]
A └ message/rfc822
 └ (forwarded=no)
B └ multipart/alternative
C └ text/plain
D └ text/html

Injected Headers

[...Cryptographic Envelope...]
D └ multipart/alternative
 └ (protected-headers=v1)
E └ text/plain
F └ text/html

(w/ legacy display)

[...Cryptographic Envelope...]
G └ multipart/mixed
 └ (protected-headers=v1)
H └ text/plain [legacy display]
 └ (protected-headers=v1)
I └ multipart/alternative
J └ text/plain
K └ text/html

only for some encrypted messages, not for signed-only messages

Header Confidentiality Policy

- When composing an **encrypted** message with header protection, how should the outside header be formed, based on the inside header?
- HCP is defined as a function in pseudocode:
 - `hcp(name, val_in) → val_out`
- (If `val_out` is null, the header name will be omitted)
- Communications tool for MUA implementers and researchers to describe their plans to each other.

Default HCP recommendation?

```
hcp_minimal(name, val_in):  
    if name is 'Subject':  
        return '[...]'  
    else:  
        return val_in
```

```
hcp_strong(name, val_in):  
    eh = ['From', 'To',  
          'Cc', 'Date']  
    if name in eh:  
        return val_in  
    elif name = 'Subject':  
        return '[...]'  
    elif name = 'Message-ID':  
        return new_message_id()  
    else:  
        return null
```

Deliverability, Server-side threading...

Confidentiality, Metadata surveillance, ...

There are other possible HCPs...

Test Vectors

<https://header-protection.cmrg.net>

imap://bob@header-protection.cmrg.net

Already evaluated with Geary

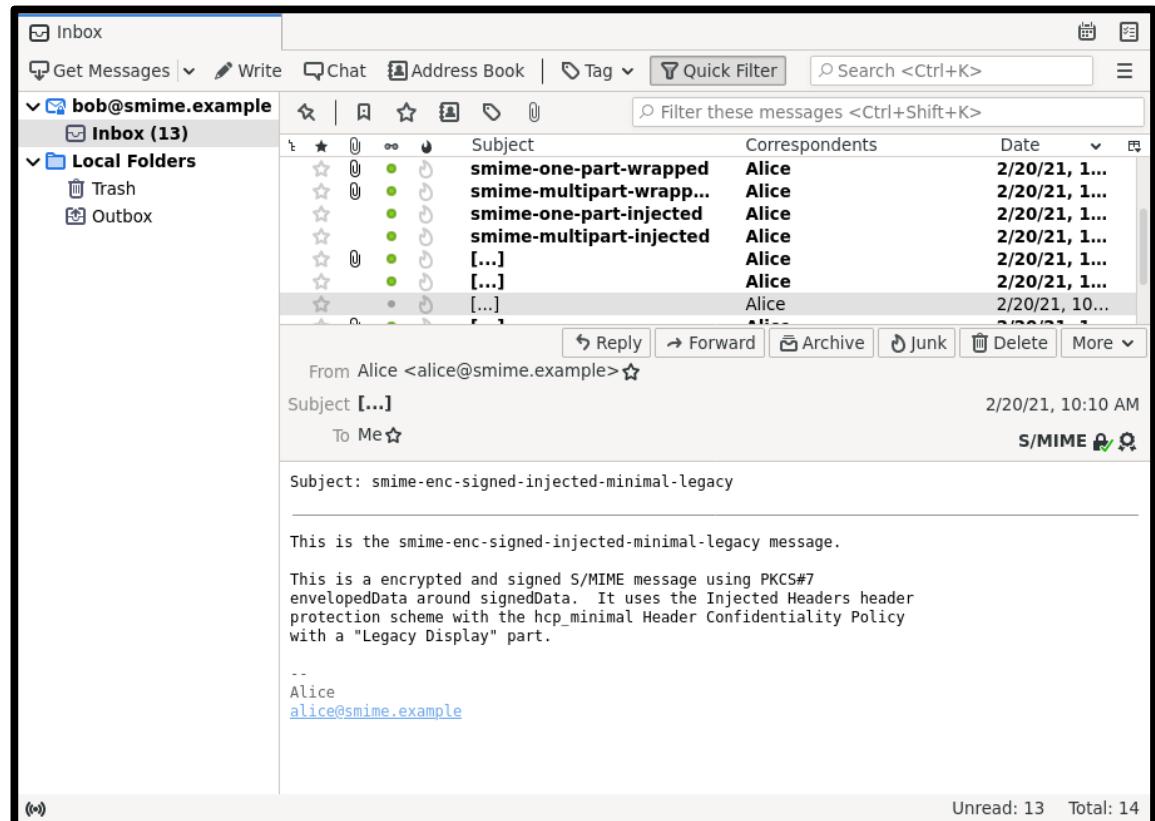


...and Thunderbird



Please point your MUA at these samples, and report!

- Legacy as well as full implementations
- Reports to spasm@ietf.org or gitlab



The screenshot shows the Thunderbird inbox for the user 'bob@smime.example'. The inbox contains 13 messages, all from 'Alice' (alice@smime.example) dated 2021-02-20. The subjects of the messages are: smime-one-part-wrapped, smime-multipart-wrapp..., smime-one-part-injected, smime-multipart-injected, [...], [...], and [...]. Below the inbox, a message from Alice is selected. The message header shows 'From Alice <alice@smime.example>' and 'Subject: [...]' with a timestamp of '2/20/21, 10:10 AM'. The message body starts with 'S/MIME' followed by a green checkmark icon. The message content is as follows:

```
This is the smime-enc-signed-injected-minimal-legacy message.  
This is an encrypted and signed S/MIME message using PKCS#7  
envelopedData around signedData. It uses the Injected Headers header  
protection scheme with the hcp_minimal Header Confidentiality Policy  
with a "Legacy Display" part.  
  
--  
Alice  
alice@smime.example
```

At the bottom of the window, it says 'Unread: 13 Total: 14'.

Help with test vectors!

-  and  not the only MUAs. Can you test?
- Why doesn't multipart/signed Wrapped Message validate?
- Generate and send test vectors through live mailservers
- What else should we evaluate?
- Messages are all simple text/plain. Need multipart/alternative? Attachments?
- HCP tests (minimal v. strong)
 - Threading?

Next Steps

- Include test vectors in -04
- Guidance for receiving side
- Guidance for replying
- Select a recommended scheme for generation
- Select a recommendation for default HCP

Choosing a scheme for message composition

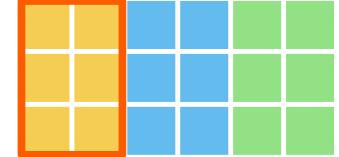
HP Scheme Evaluation

Protections for composed Message

| | | Recipient MUA Capabilities | | | |
|----------------------------------|--------------------------------|----------------------------|-----------------------------|--------------------------|-------------------------|
| | | Legacy (no crypto) render | Legacy (with crypto) render | Fully Implemented render | Fully Implemented reply |
| Protections for composed Message | Signed-only (multipart/signed) | | | | good |
| | Signed-only (pkcs7 signedData) | unreadable message | unreadable message | good | good |
| | Signed & encrypted | unreadable message | unreadable message | good | good |



Geary 3.38.1 (Legacy, Non-Crypto)



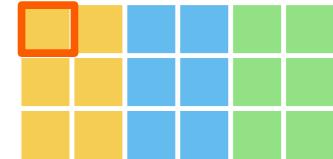
Configuration

Add an account Create

| | |
|---------------|----------------------------|
| Your name | Bob |
| Email address | bob@smime.example |
| Receiving | |
| IMAP server | header-protection.cmrg.net |
| Login name | bob |
| Password | |
| Sending | |
| SMTP server | localhost |



Geary 3.38.1 (Legacy, Non-Crypto)



Multipart/Signed render

This screenshot shows the Geary interface with an inbox containing two messages from Alice. The top message is a wrapped S/MIME message, and the bottom message is a standard multipart message. The message body contains the text: "This is the smime-multipart-wrapped message. This is a signed-only S/MIME message via PKCS#7 detached signature (multipart/signed). It uses the Wrapped Message header protection scheme." Below the message body, there is a quoted section from Alice and download links for the message and its signature.

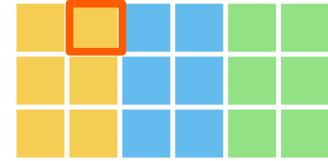
Wrapped Message

This screenshot shows the Geary interface with an inbox containing a single message from Alice. The message is an injected headers S/MIME message. The message body contains the text: "This is the smime-multipart-injected message. This is a signed-only S/MIME message via PKCS#7 detached signature (multipart/signed). It uses the Injected Headers header protection scheme." Below the message body, there is a quoted section from Alice and download links for the message and its signature.

Injected Headers



Geary 3.38.1 (Legacy, Non-Crypto)



Multipart/Signed reply

The screenshot shows the Geary application interface. The left sidebar displays an inbox with 17 messages, including one from Alice. The main window shows a reply message from Alice. The message content starts with a quoted section: "On Sat, Feb 20, 2021 at 10:05, Alice <alice@smime.example> wrote:". Below this, the message body contains the text "smime-one-part-wrapped". The message is signed by Alice, with the signature "Alice smime-multipart-wrapped" visible at the bottom.

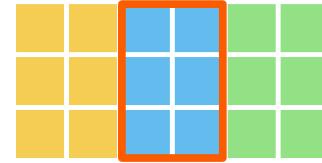
The screenshot shows the Geary application interface. The left sidebar displays an inbox with 17 messages, including one from Alice. The main window shows a reply message from Alice. The message content starts with a quoted section: "On Sat, Feb 20, 2021 at 10:07, Alice <alice@smime.example> wrote: This is the smime-multipart-injected message." Below this, the message body contains the text "smime-multipart-injected. This is the smime-multipart-injected message. This is a signed...". The message is signed by Alice, with the signature "Alice alice@smime.example" visible at the bottom.

Wrapped Message

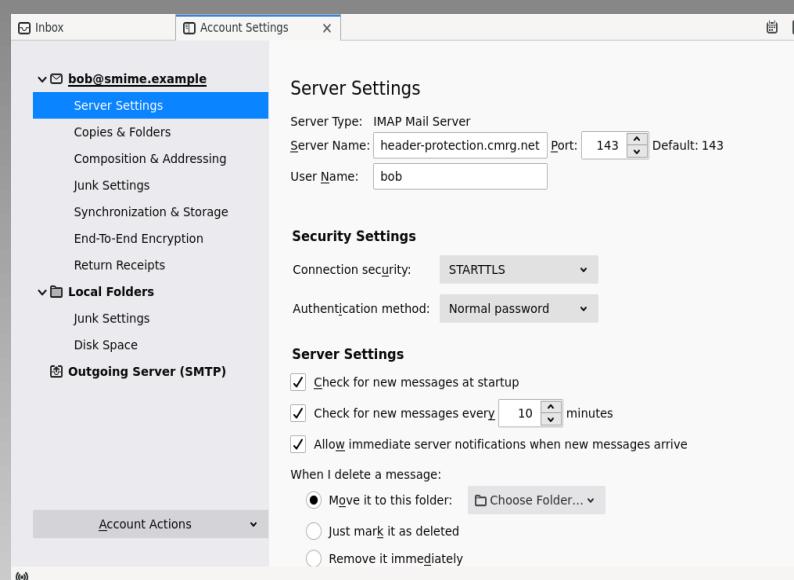
Injected Headers



Thunderbird 78.8.0 (Legacy, Crypto-capable)

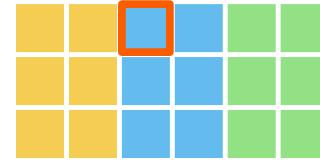


Configuration





Thunderbird 78.8.0 (Legacy, Crypto-capable)



Multipart/Signed render

Inbox

Get Messages | Write Chat Address Book Tag Quick Filter Search <Ctrl+K>

bob@smime.example

- Inbox (13)
- Local Folders
 - Trash
 - Outbox

Filter these messages <Ctrl+Shift+K>

| | Subject | Correspondents | Date |
|---|--------------------------|----------------|----------------|
| ★ | smime-enc-signed | Alice | 2/20/21, 1... |
| ★ | smime-one-part-wrapped | Alice | 2/20/21, 1... |
| ★ | smime-multipart-wrapped | Alice | 2/20/21, 10... |
| ★ | smime-one-part-injected | Alice | 2/20/21, 1... |
| ★ | smime-multipart-injected | Alice | 2/20/21, 1... |
| ★ | [...] | Alice | 2/20/21, 1... |
| ★ | [...] | Alice | 2/20/21, 1... |
| ★ | [...] | Alice | 2/20/21, 1... |
| ★ | [...] | Alice | 2/20/21, 1... |
| ★ | [...] | Alice | 2/20/21, 1... |
| ★ | [...] | Alice | 2/20/21, 1... |

From Alice <alice@smime.example>★
Subject: smime-multipart-wrapped
To Me★
S/MIME

—smime-multipart-wrapped.eml—
Subject: smime-multipart-wrapped
From: Alice <alice@smime.example>
Date: 2/20/21, 10:05 AM
To: Bob <bob@smime.example>

This is the smime-multipart-wrapped message.

This is a signed-only S/MIME message via PKCS#7 detached signature (multipart/signed). It uses the Wrapped Message header protection scheme.

> 1 attachment: smime-multipart-wrapped.eml 495 bytes

Save Unread: 13 Total: 14

Inbox

Get Messages | Write Chat Address Book Tag Quick Filter Search <Ctrl+K>

bob@smime.example

- Inbox (13)
- Local Folders
 - Trash
 - Outbox

Filter these messages <Ctrl+Shift+K>

| | Subject | Correspondents | Date |
|---|--------------------------|----------------|----------------|
| ★ | smime-enc-signed | Alice | 2/20/21, 1... |
| ★ | smime-one-part-wrapped | Alice | 2/20/21, 1... |
| ★ | smime-multipart-wrapp... | Alice | 2/20/21, 1... |
| ★ | smime-one-part-injected | Alice | 2/20/21, 1... |
| ★ | smime-multipart-injected | Alice | 2/20/21, 10... |
| ★ | [...] | Alice | 2/20/21, 1... |
| ★ | [...] | Alice | 2/20/21, 1... |
| ★ | [...] | Alice | 2/20/21, 1... |

From Alice <alice@smime.example>★
Subject: smime-multipart-injected
To Me★
S/MIME

This is the smime-multipart-injected message.

This is a signed-only S/MIME message via PKCS#7 detached signature (multipart/signed). It uses the Injected Headers header protection scheme.

—
Alice
alice@smime.example

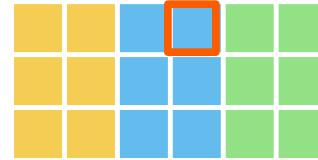
Unread: 13 Total: 14

Wrapped Message

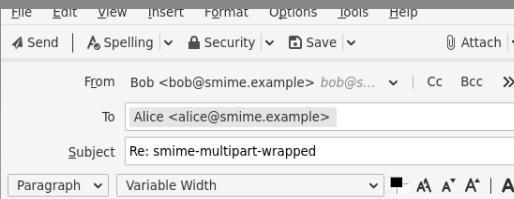
Injected Headers



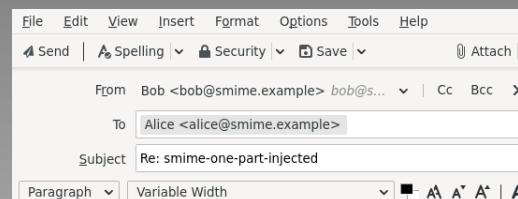
Thunderbird 78.8.0 (Legacy, Crypto-capable)



Multipart/Signed reply



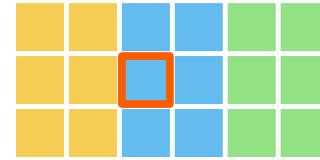
Wrapped Message



Injected Headers



Thunderbird 78.8.0 (Legacy, Crypto-capable)



Signed (S/MIME signedData) render

Inbox

Get Messages | Write Chat Address Book Tag Quick Filter Search <Ctrl+K>

bob@smime.example

Inbox (13)

Local Folders

Trash Outbox

Filter these messages <Ctrl+Shift+K>

| | Subject | Correspondents | Date |
|------|--------------------------|----------------|----------------|
| star | smime-enc-signed | Alice | 2/20/21, 1... |
| star | smime-one-part-wrapped | Alice | 2/20/21, 10... |
| star | smime-multipart-wrap... | Alice | 2/20/21, 1... |
| star | smime-one-part-injected | Alice | 2/20/21, 1... |
| star | smime-multipart-injected | Alice | 2/20/21, 1... |
| star | [...] | Alice | 2/20/21, 1... |
| star | [...] | Alice | 2/20/21, 1... |
| star | [...] | Alice | 2/20/21, 1... |
| star | [...] | Alice | 2/20/21, 1... |
| star | [...] | Alice | 2/20/21, 1... |
| star | [...] | Alice | 2/20/21, 1... |
| star | [...] | Alice | 2/20/21, 1... |

From Alice <alice@smime.example>☆

Subject smime-one-part-wrapped

To Me ☆

S/MIME

—smime-one-part-wrapped.eml—

Subject: smime-one-part-wrapped

From: Alice <alice@smime.example>

Date: 2/20/21, 10:04 AM

To: Bob <bob@smime.example>

This is the smime-one-part-wrapped message.

This is a signed-only S/MIME message via PKCS#7 signedData. It uses the Wrapped Message header protection scheme.

> 0 1 attachment: smime-one-part-wrapped.eml 465 bytes

Save Unread: 13 Total: 14

Inbox

Get Messages | Write Chat Address Book Tag Quick Filter Search <Ctrl+K>

bob@smime.example

Inbox (13)

Local Folders

Trash Outbox

Filter these messages <Ctrl+Shift+K>

| | Subject | Correspondents | Date |
|------|--------------------------|----------------|----------------|
| star | smime-enc-signed | Alice | 2/20/21, 1... |
| star | smime-one-part-wrapped | Alice | 2/20/21, 1... |
| star | smime-multipart-wrap... | Alice | 2/20/21, 1... |
| star | smime-one-part-injected | Alice | 2/20/21, 10... |
| star | smime-multipart-injected | Alice | 2/20/21, 1... |
| star | [...] | Alice | 2/20/21, 1... |
| star | [...] | Alice | 2/20/21, 1... |
| star | [...] | Alice | 2/20/21, 1... |
| star | [...] | Alice | 2/20/21, 1... |
| star | [...] | Alice | 2/20/21, 1... |
| star | [...] | Alice | 2/20/21, 1... |

From Alice <alice@smime.example>☆

Subject smime-one-part-injected

To Me ☆

This is the smime-one-part-injected message.

This is a signed-only S/MIME message via PKCS#7 signedData. It uses the Injected Headers header protection scheme.

—Alice
alice@smime.example

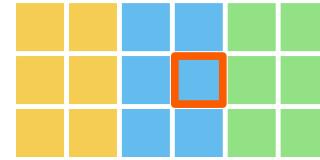
Unread: 13 Total: 14

Wrapped Message

Injected Headers



Thunderbird 78.8.0 (Legacy, Crypto-capable)



Signed (SMIME signedData) reply

The image shows two side-by-side Thunderbird message windows. Both windows have the following header information:

- File
- Edit
- View
- Insert
- Format
- Options
- Tools
- Help

Toolbar buttons include:

- Send
- Spelling
- Security
- Save
- Attach

Message details:

- From: Bob <bob@smime.example>
- To: Alice <alice@smime.example>
- Subject: Re: smime-one-part-wrapped

Content pane (Wrapped Message):

On 2/20/21 10:04 AM, Alice wrote:
This is the smime-one-part-injected message.
This is a signed-only S/MIME message via PKCS#7 signedData. It uses the Injected Headers header protection scheme.

Message details (Injected Headers):

- From: Bob <bob@smime.example>
- To: Alice <alice@smime.example>
- Subject: Re: smime-one-part-injected

Content pane (Injected Headers):

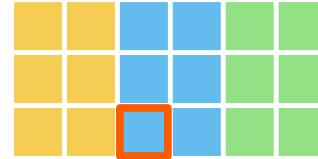
On 2/20/21 10:06 AM, Alice wrote:
This is the smime-one-part-injected message.
This is a signed-only S/MIME message via PKCS#7 signedData. It uses the Injected Headers header protection scheme.

Wrapped Message

Injected Headers



Thunderbird 78.8.0 (Legacy, Crypto-capable)



Encrypted + Signed render

This screenshot shows the Thunderbird inbox with an encrypted and signed message from Alice. The message is titled "smime-enc-signed-wrapped-minimal.eml". The message body contains the following text:

```
From: Alice <alice@smime.example>
Subject: [...]
To: Me ☆
```

The message is marked as "S/MIME" and has a small padlock icon.

This screenshot shows the Thunderbird inbox with an encrypted and signed message from Alice. The message is titled "smime-enc-signed-wrapped-minimal.eml". The message body contains the following text:

```
From: Alice <alice@smime.example>
Subject: [...]
To: Me ☆
```

The message is marked as "S/MIME" and has a small padlock icon. Below the message, there is a note: "This is the smime-enc-signed-injected-minimal message. This is an encrypted and signed S/MIME message using PKCS#7 envelopedData around signedData. It uses the Wrapped Message header protection scheme with the hcp_minimal Header Confidentiality Policy."

This screenshot shows the Thunderbird inbox with an encrypted and signed message from Alice. The message is titled "smime-enc-signed-wrapped-minimal.eml". The message body contains the following text:

```
From: Alice <alice@smime.example>
Subject: [...]
To: Me ☆
```

The message is marked as "S/MIME" and has a small padlock icon. Below the message, there is a note: "This is the smime-enc-signed-injected-minimal-legacy message. This is a encrypted and signed S/MIME message using PKCS#7 envelopedData around signedData. It uses the Injected Headers header protection scheme with the hcp_minimal Header Confidentiality Policy with a 'Legacy Display' part."

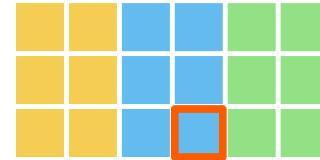
Wrapped Message

Injected Headers
w/o Legacy Display

Injected Headers
w/ Legacy Display



Thunderbird 78.8.0 (Legacy, Crypto-capable)



Encrypted + Signed reply

The figure displays three Thunderbird windows side-by-side, each showing a different way to handle S/MIME encrypted and signed messages.

- Wrapped Message:** The first window shows the message content wrapped directly in the body. It includes the recipient's name, the subject, and the message text "On 2/20/21 10:08 AM, Alice wrote:". A small S/MIME icon with a lock is visible at the bottom.
- Injected Headers w/o Legacy Display:** The second window shows the message content with injected headers. It includes the recipient's name, the subject, and the message text "On 2/20/21 10:09 AM, Alice wrote:". Below the message, there is a note: "This is the smime-enc-signed-injected-minimal message. This is a encrypted and signed S/MIME message using PKCS#7 envelopedData around signedData. It uses the Injected Headers header protection scheme with the hcp_minimal Header Confidentiality Policy." A small S/MIME icon with a lock is visible at the bottom.
- Injected Headers w/ Legacy Display:** The third window shows the message content with injected headers and legacy display. It includes the recipient's name, the subject, and the message text "On 2/20/21 10:10 AM, Alice wrote:". Below the message, there is a note: "Subject: smime-enc-signed-injected-minimal-legacy This is the smime-enc-signed-injected-minimal-legacy message. This is a encrypted and signed S/MIME message using PKCS#7 envelopedData around signedData. It uses the Injected Headers header protection scheme with the hcp_minimal Header Confidentiality Policy with a "Legacy Display" part." A small S/MIME icon with a lock is visible at the bottom.

Wrapped Message

Injected Headers w/o Legacy Display

Injected Headers w/ Legacy Display