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
```

Deliverability, Server-side threading...

```
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
```

Confidentiality, Metadata surveillance, ...

There are other possible HCPs...

Test Vectors

https://header-protection.cmrg.net

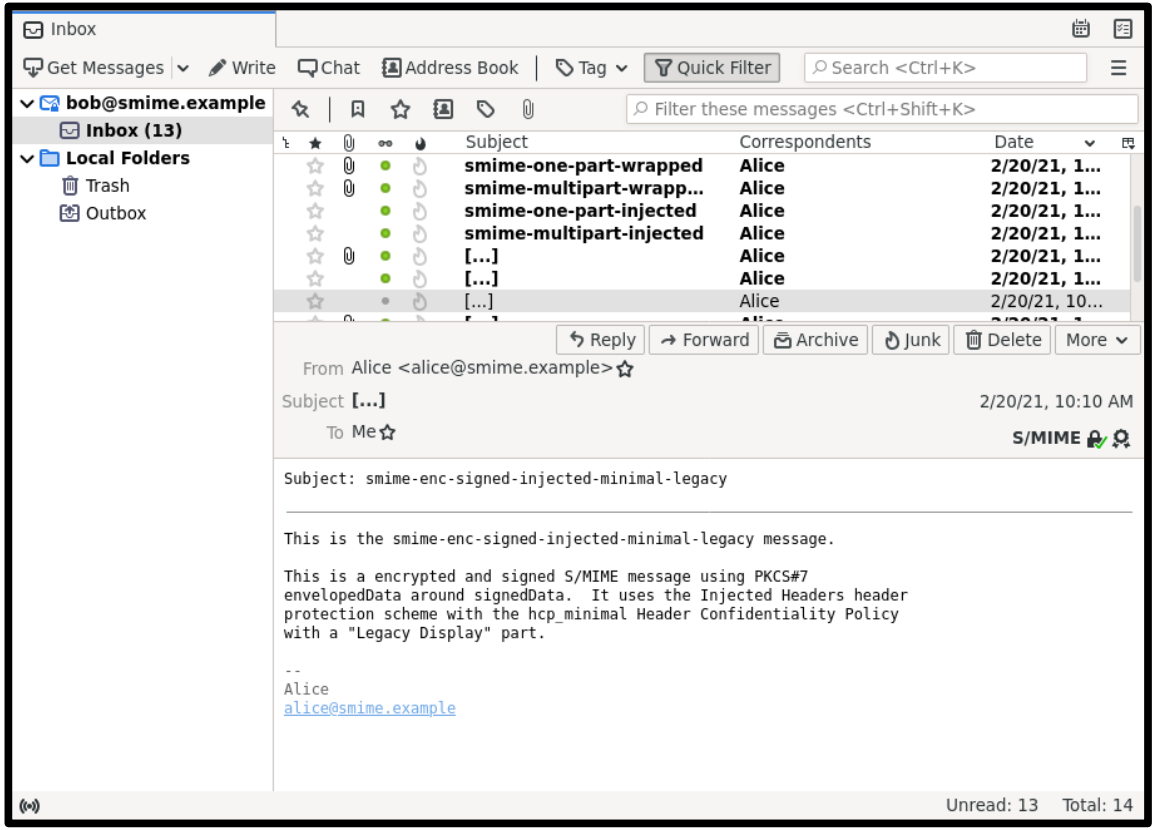
imap://bob@header-protection.cmrg.net

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



Help with test vectors!

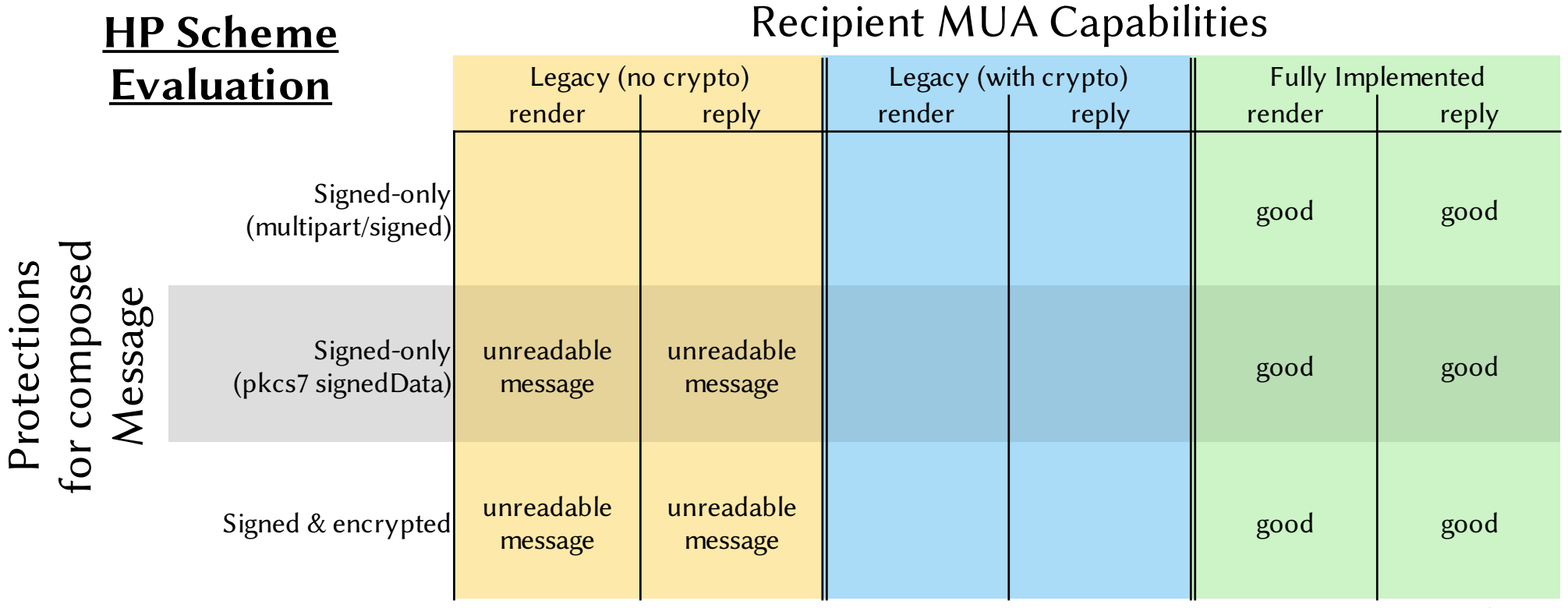
-  and  not the only MUAs. Can you test?
- Why doesn't multipart/signed Wrapped Message validate?
- Generate and send test vectors through live mailservers
- What else should we evaluate?
- Messages are all simple text/plain. Need multipart/alternative? Attachments?
- HCP tests (minimal v. strong)
 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

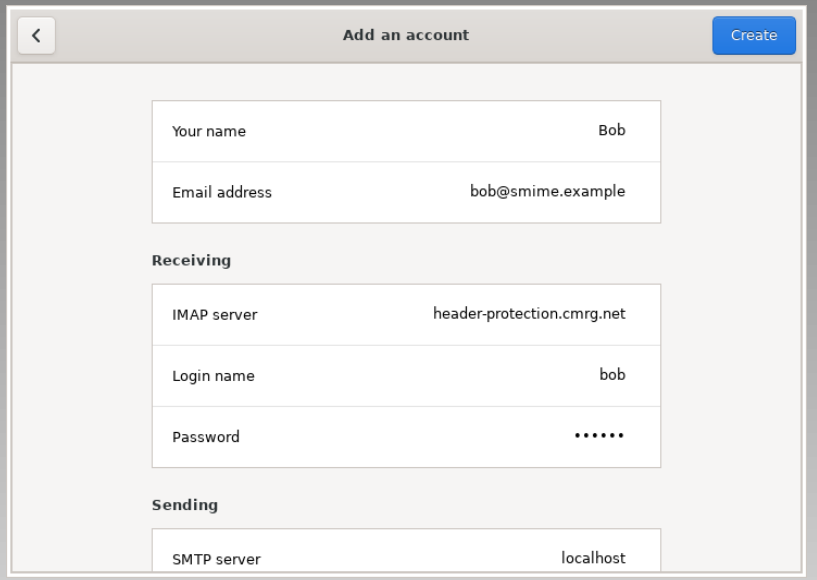
Choosing a scheme for message composition

HP Scheme Evaluation



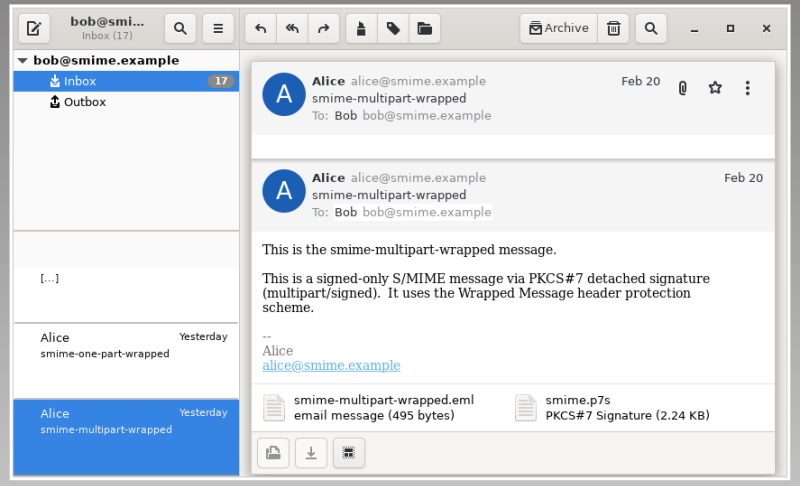
Geary 3.38.1 (Legacy, Non-Crypto)

Configuration

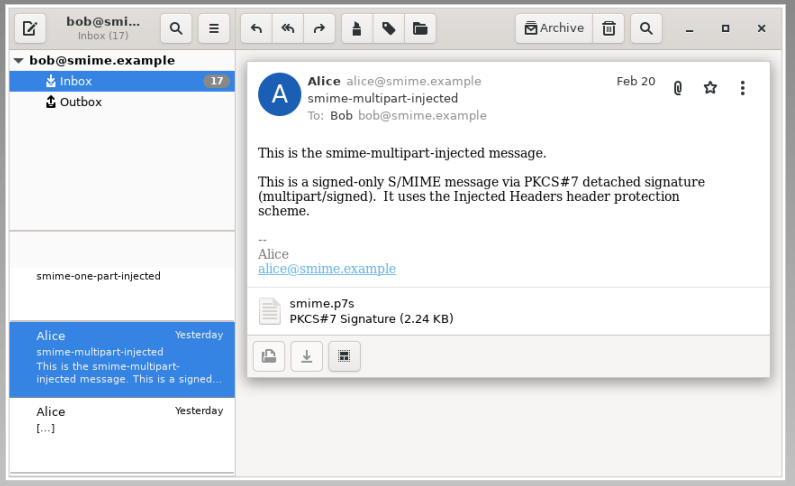


Geary 3.38.1 (Legacy, Non-Crypto)

Multipart/Signed render



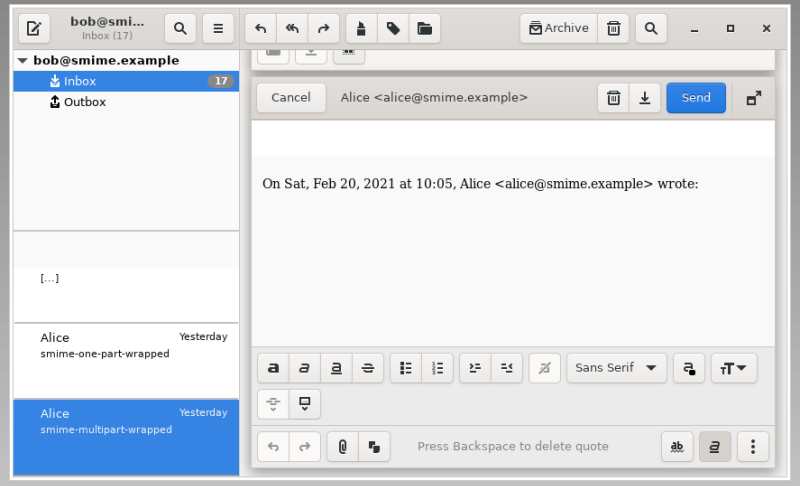
Wrapped Message



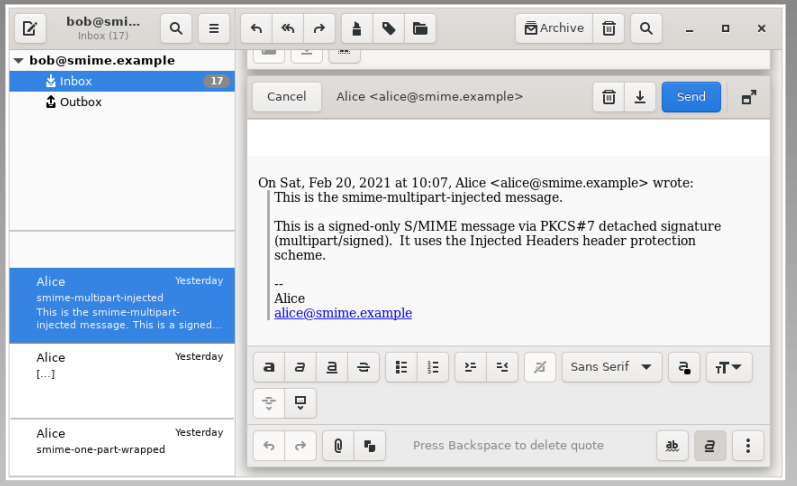
Injected Headers

Geary 3.38.1 (Legacy, Non-Crypto)

Multipart/Signed reply



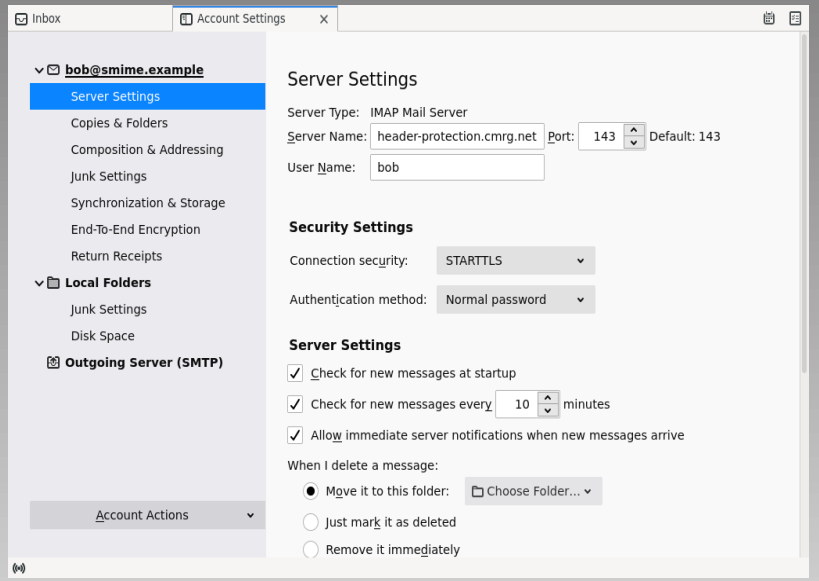
Wrapped Message



Injected Headers

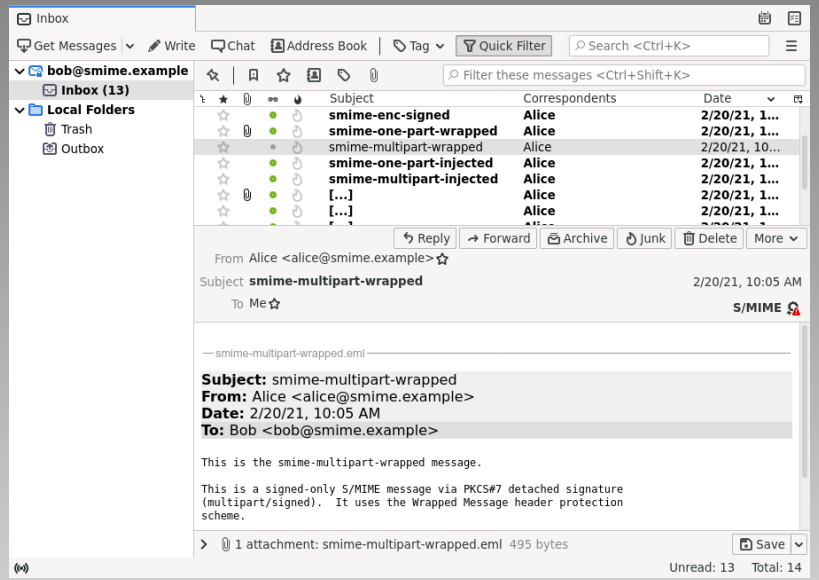
Thunderbird 78.8.0 (Legacy, Crypto-capable)

Configuration

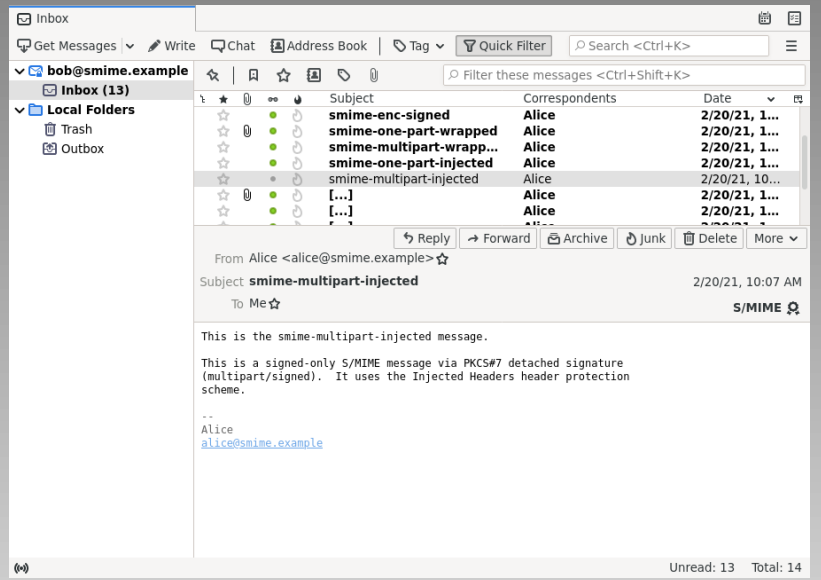


Thunderbird 78.8.0 (Legacy, Crypto-capable)

Multipart/Signed render



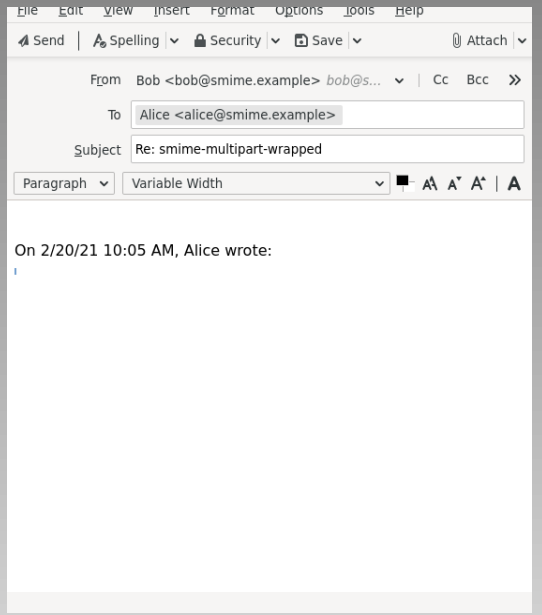
Wrapped Message



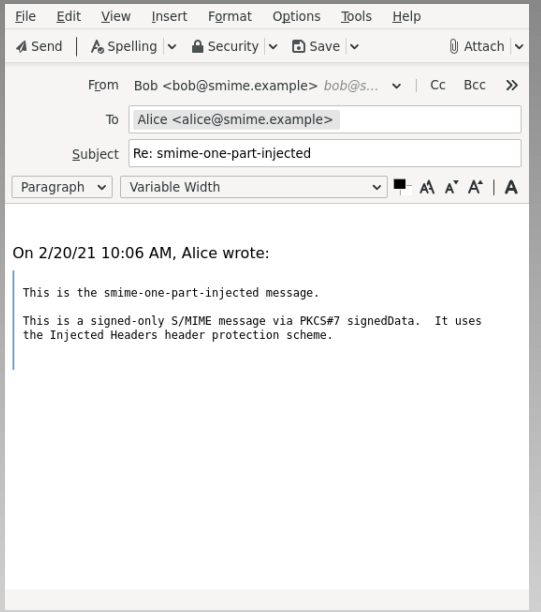
Injected Headers

Thunderbird 78.8.0 (Legacy, Crypto-capable)

Multipart/Signed reply



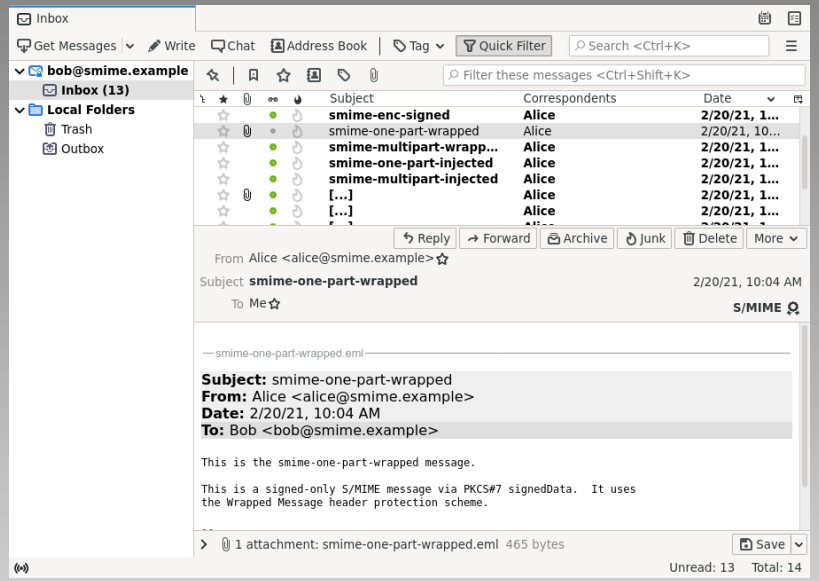
Wrapped Message



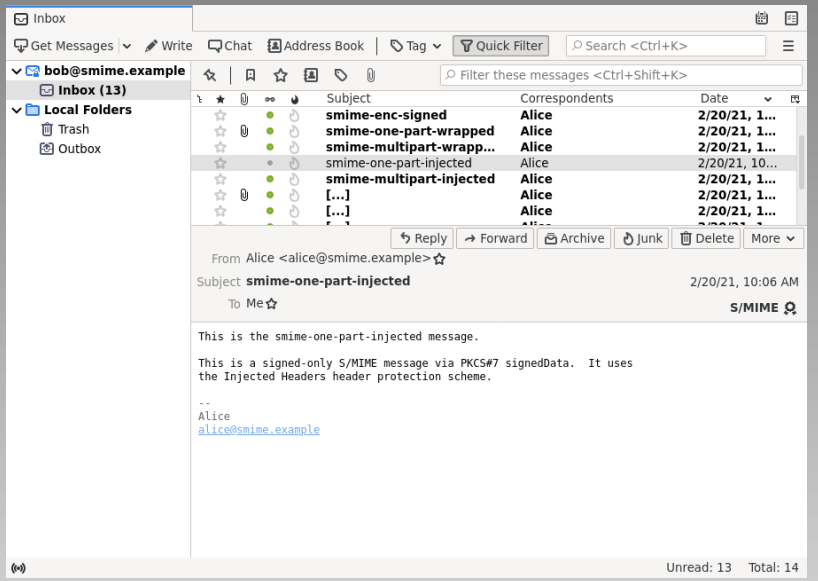
Injected Headers

Thunderbird 78.8.0 (Legacy, Crypto-capable)

Signed (SMIME signedData) render



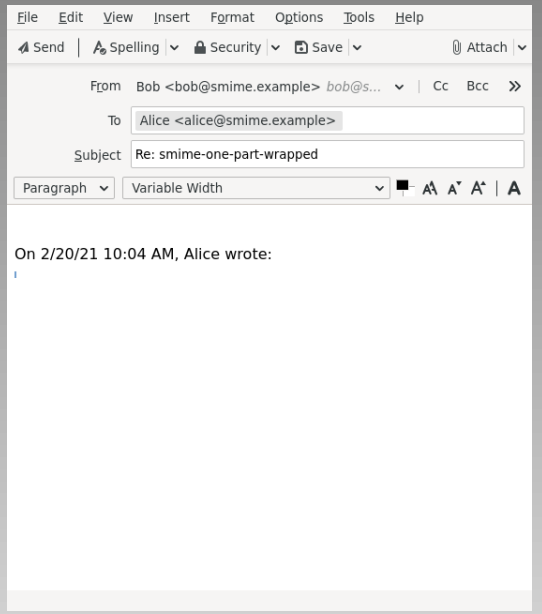
Wrapped Message



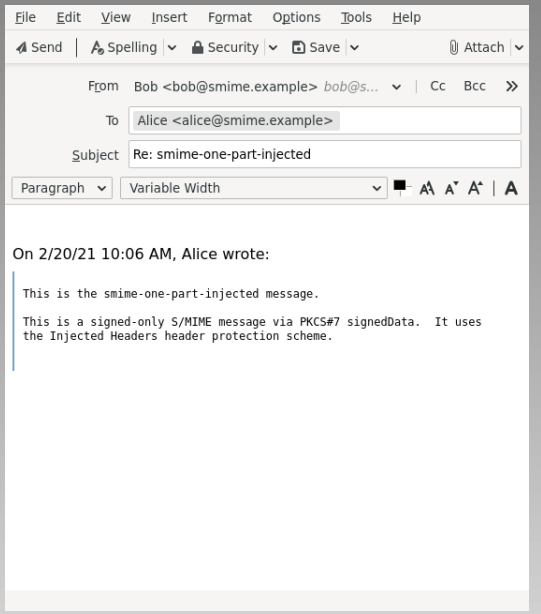
Injected Headers

Thunderbird 78.8.0 (Legacy, Crypto-capable)

Signed (SMIME signedData) reply



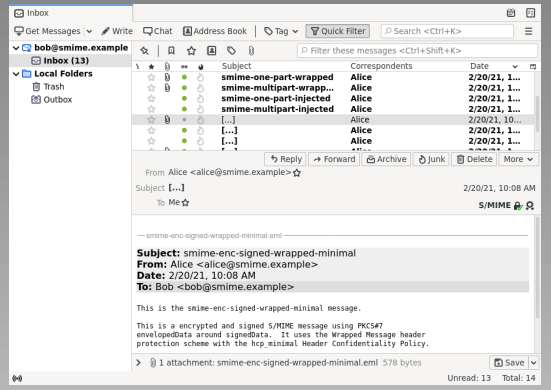
Wrapped Message



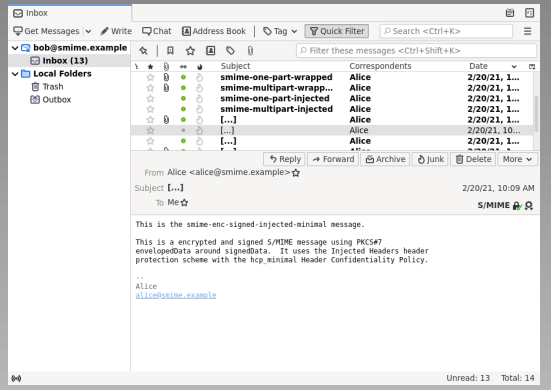
Injected Headers

Thunderbird 78.8.0 (Legacy, Crypto-capable)

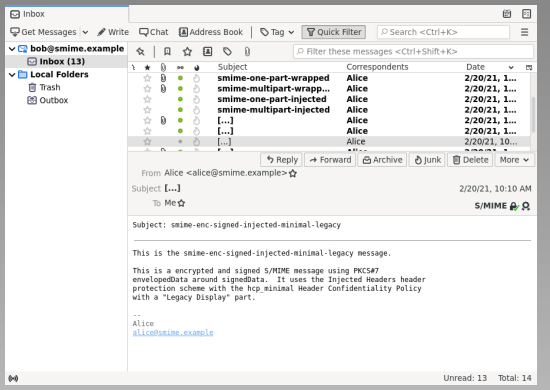
Encrypted + Signed render



Wrapped Message



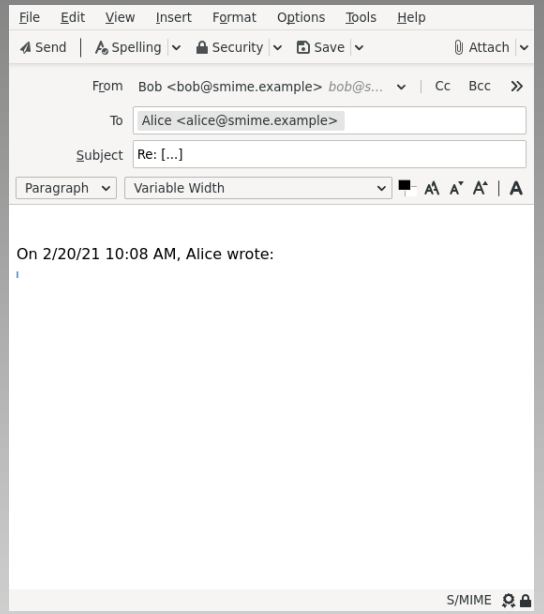
Injected Headers
w/o Legacy Display



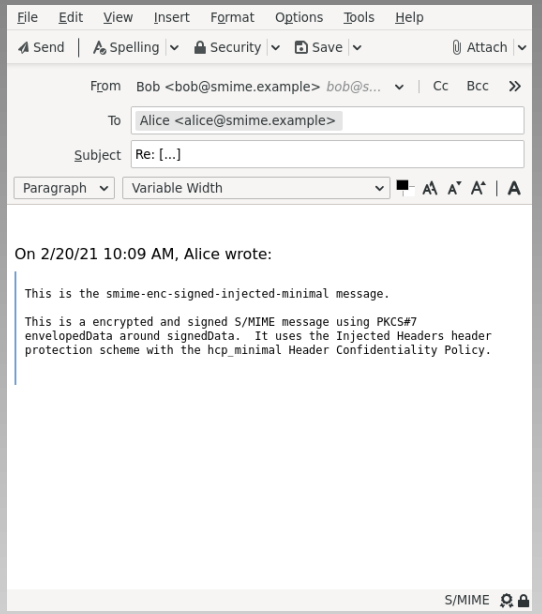
Injected Headers
w/ Legacy Display

Thunderbird 78.8.0 (Legacy, Crypto-capable)

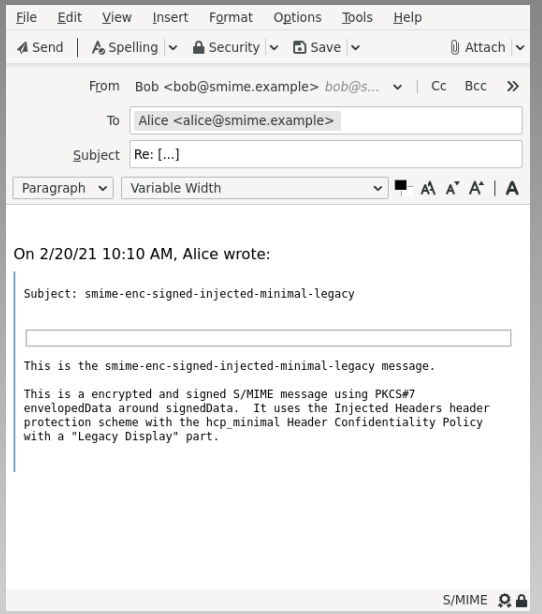
Encrypted + Signed reply



Wrapped Message



Injected Headers w/o Legacy Display



Injected Headers w/ Legacy Display