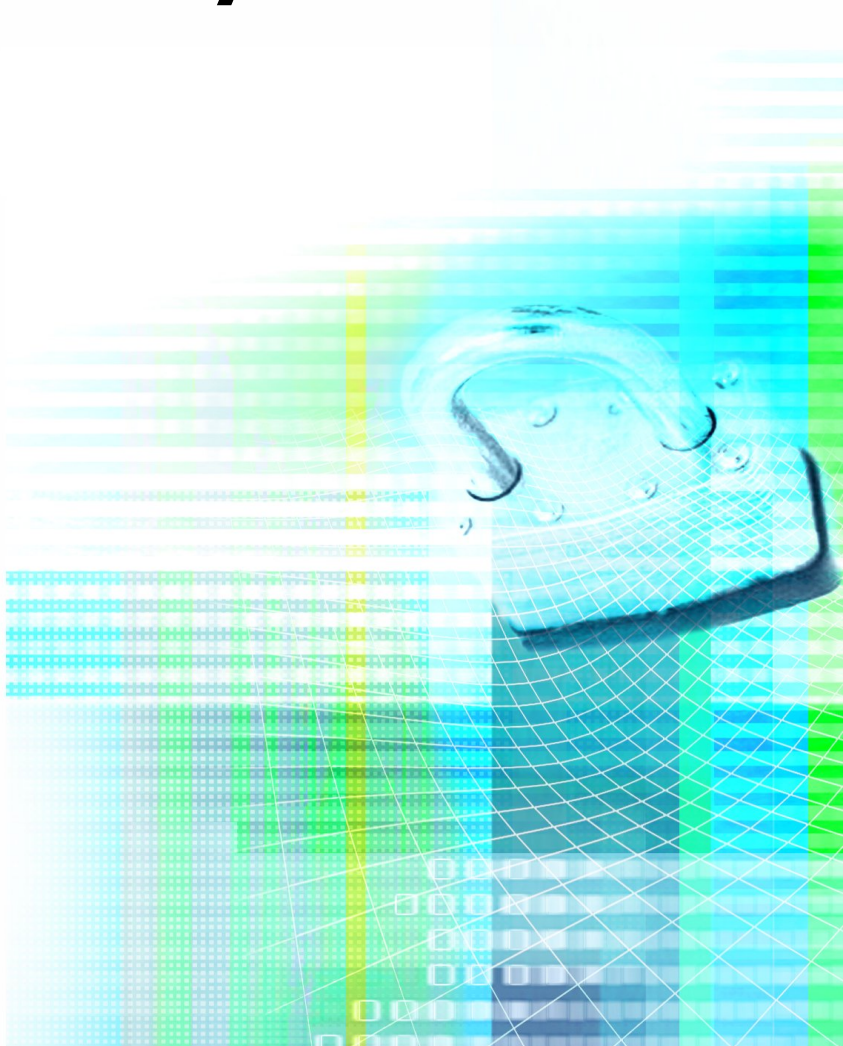
X-ARF: End-to-End Security with S/MIME and PGP/MIME

27.09.2012
TF-CSIRT, Ljubljana

Tilmann Haak
Sven Übelacker
Torsten Voss

DFN-CERT Services GmbH
Hamburg



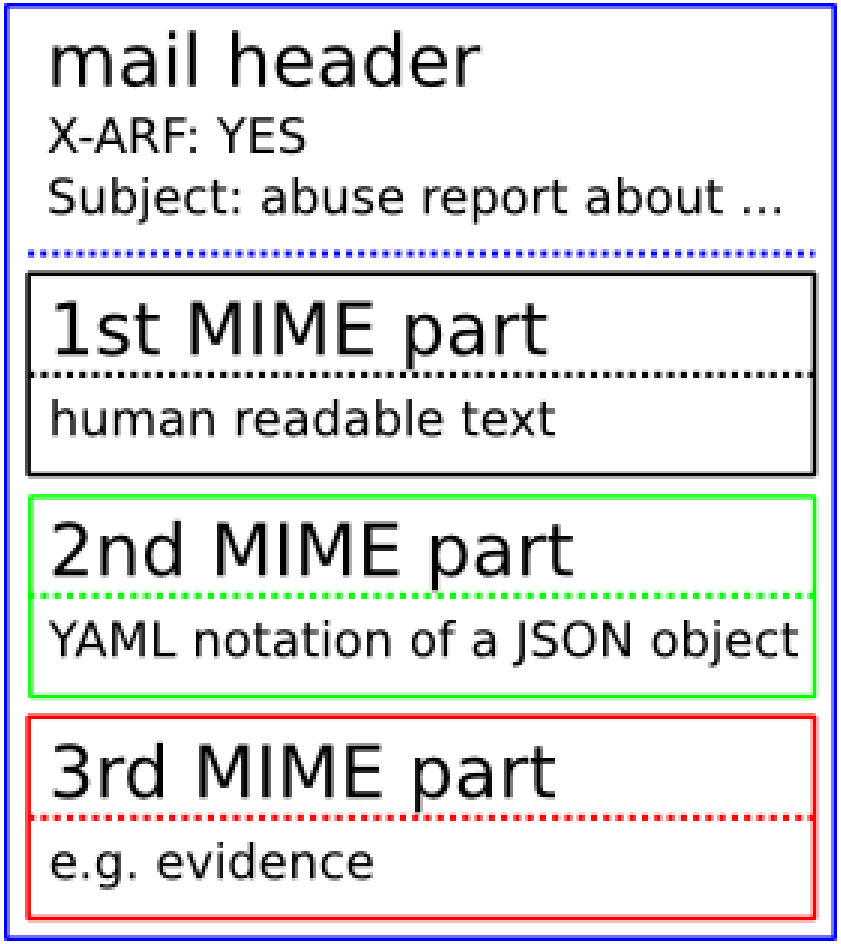
Agenda

- Motivation
- Chosen approach
- Current proposal
- Examples
- Discussion

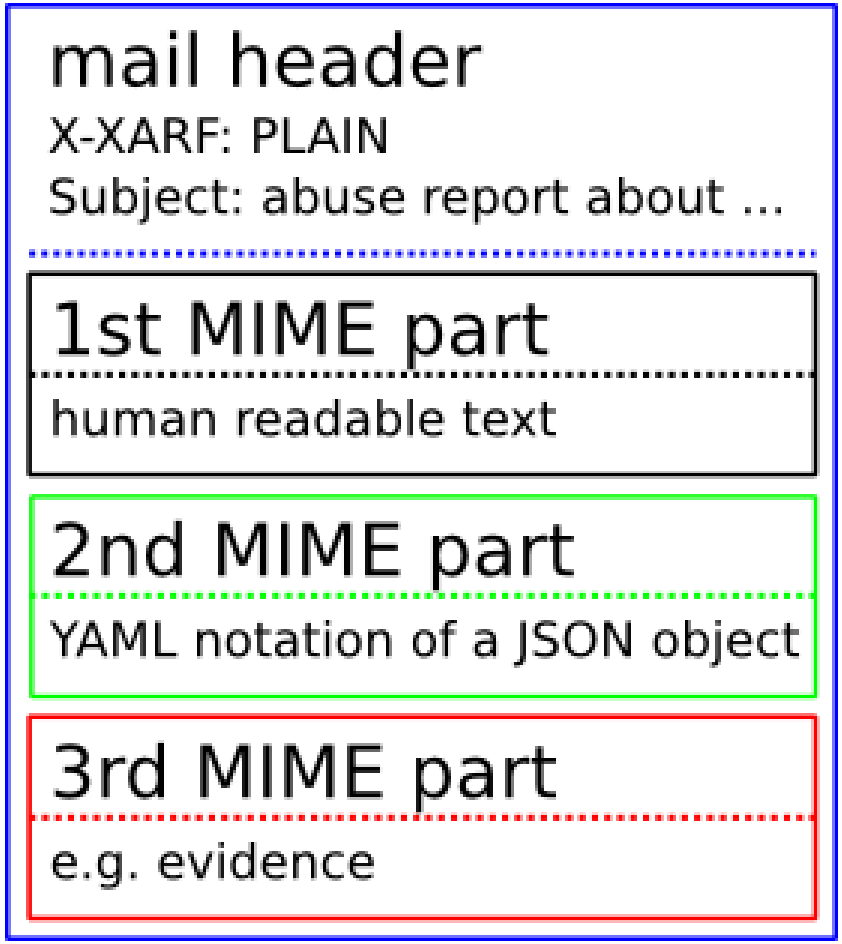
Motivation

- End-to-end security for X-ARF messages
- Keep up the X-ARF idea
  - Simple
  - Human- and machine readable
  - Use of existing standards
- The proposed extension is completely **optional**
- Exclude complicated variants
- Easy processing
- Backward compatible

X-ARF v0.1 / X-ARF v0.2



X-ARF v0.1



X-ARF v0.2 (PLAIN)

Possible Approaches

- Two basic standards:
  - S/MIME (X.509)
  - PGP/MIME

a) Just sign or encrypt a plain X-ARF message
   → Different MIME structures

b) Sign or encrypt a container
   → Some overhead

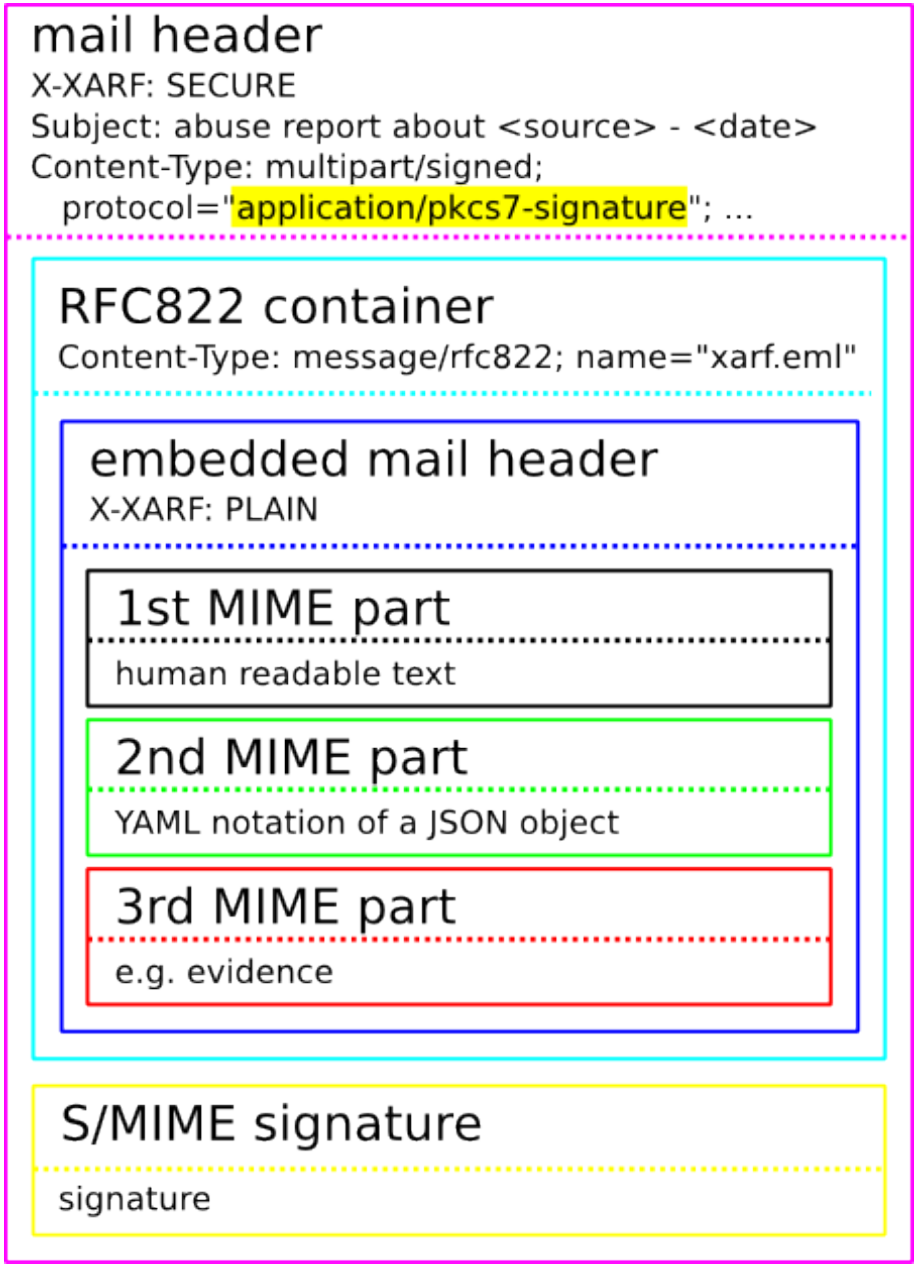
X-ARF v0.1 or v0.2?

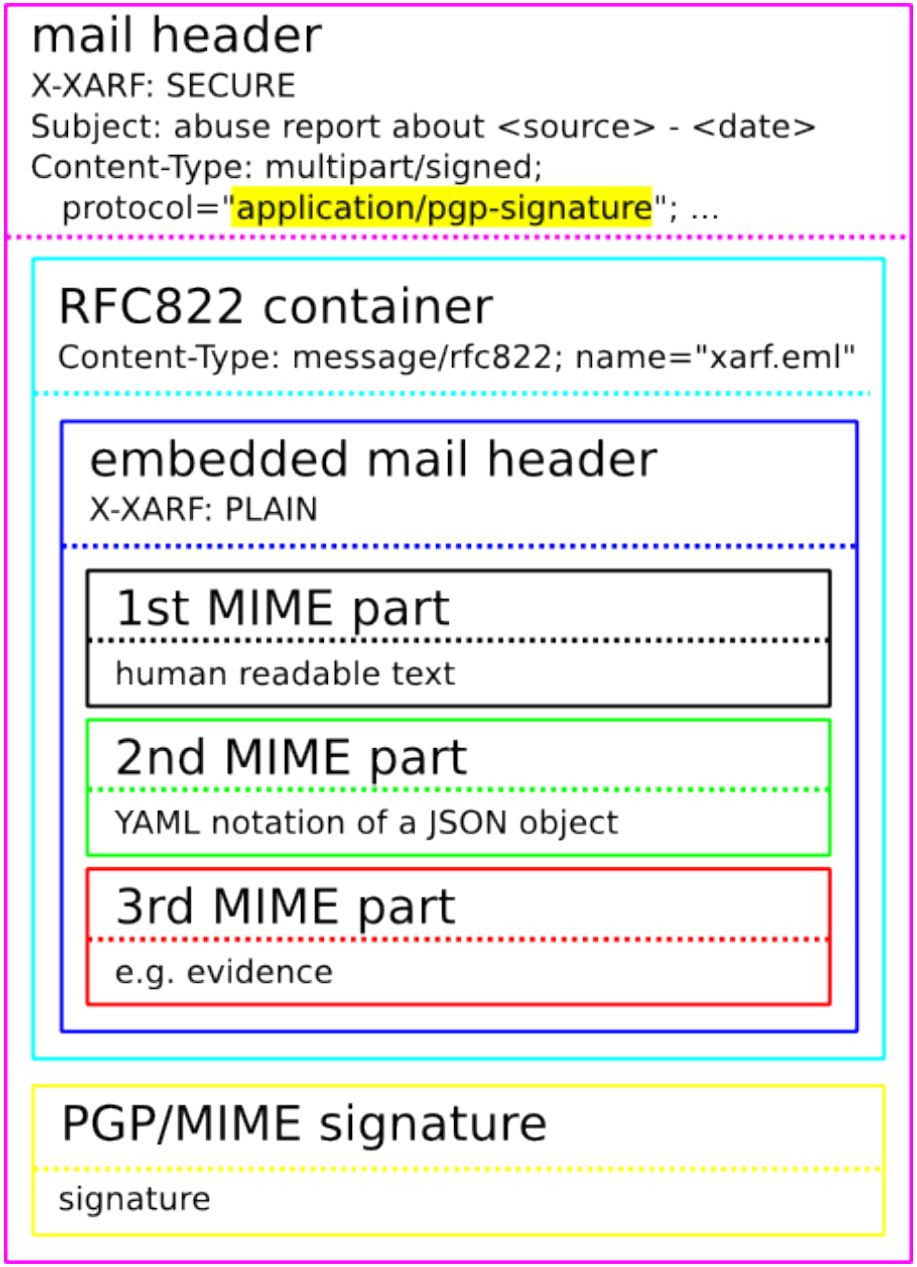
- X-ARF v0.1 and v0.2 may easily be distinguished between:
  - X-ARF: YES indicates X-ARF v0.1
  - X-XARF: PLAIN or SECURE indicates X-ARF v0.2
- No changes needed for old (v0.1) importers or exporters

X-ARF v0.2 (Proposal)

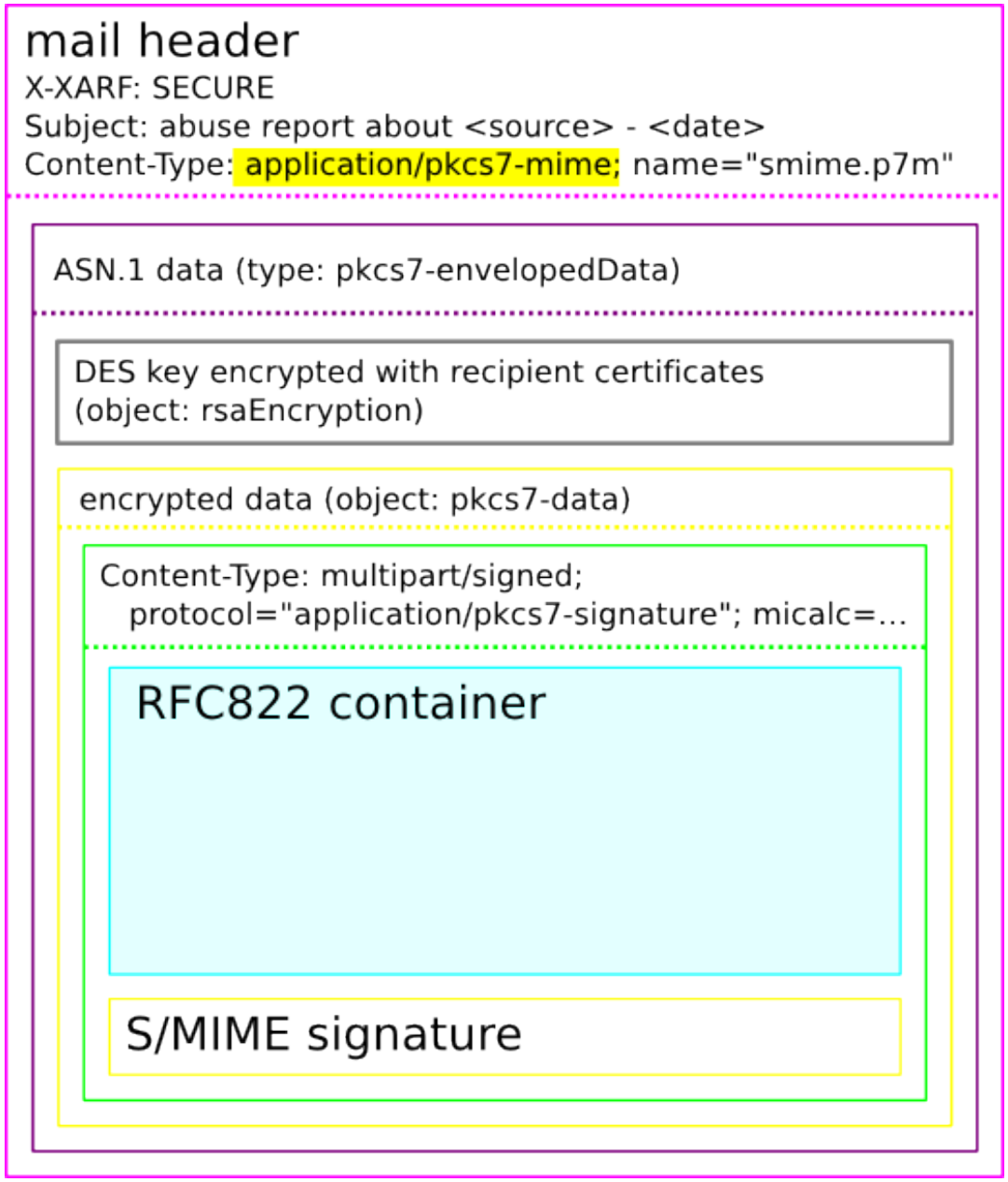
- Plain X-ARF is marked as „X-XARF: PLAIN“ in the e-mail header
- „X-XARF: SECURE“ indicates that an RFC822 container signed and/or encrypted with either S/MIME or PGP/MIME is following
- The container itself is just a normal X-ARF message (named as „xarf.eml“)
- New Content-Types multipart/signed (RFC 1847), multipart/encrypted (RFC 1847) and application/pkcs7-mime (RFC 5751)
- multipart/mixed is still the default

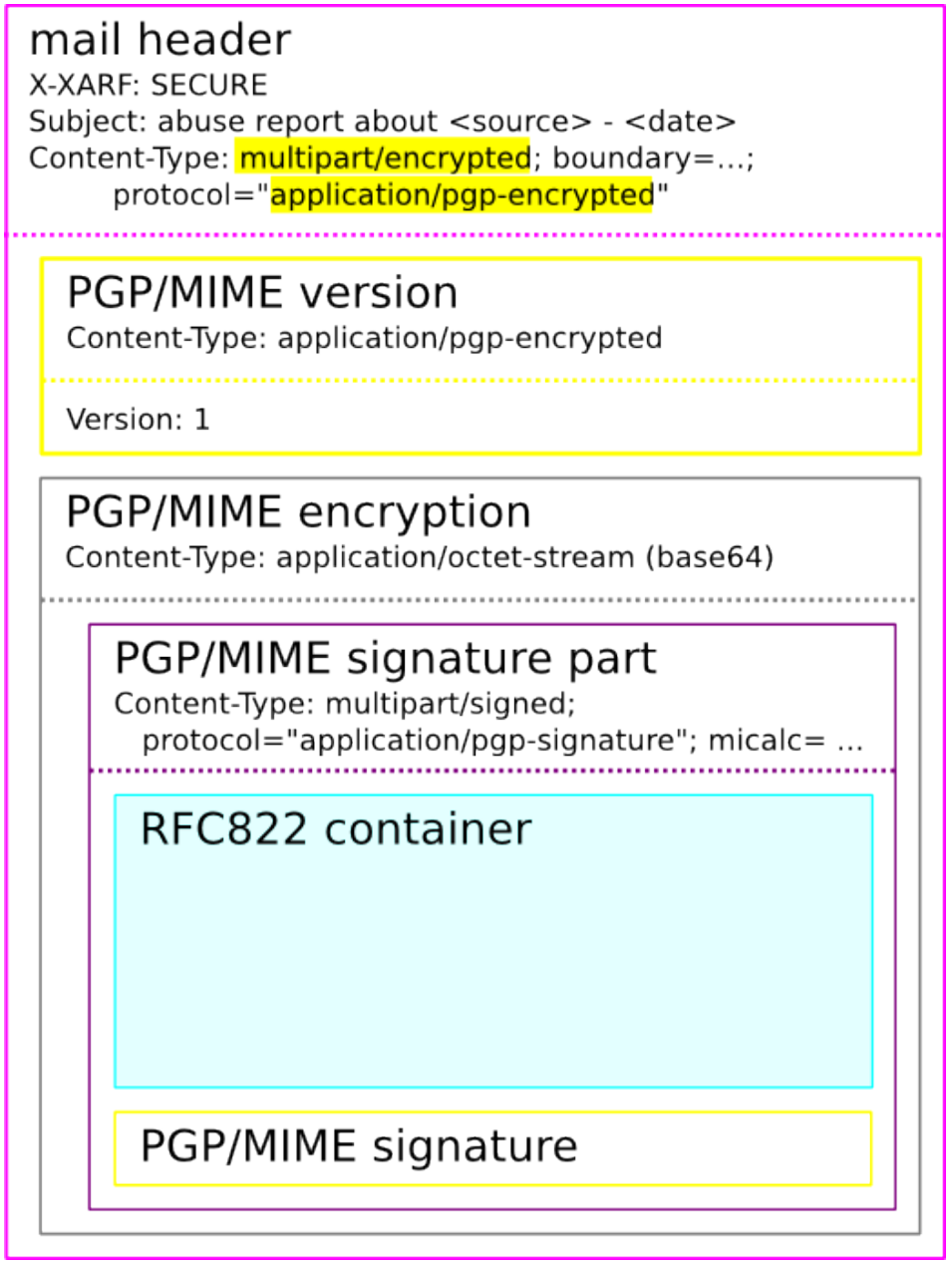
X-XARF: SECURE (signed)





X-XARF: SECURE (sig + enc)





X-XARF: SECURE

- S/MIME and PGP/MIME are using different Content-Types
- multipart/signed is used for messages signed with S/MIME and PGP/MIME
- The protocol type is used to tell them apart:
  - application/pkcs7-signature (RFC 5751)
  - application/pgp-signature (RFC 3156)

Questions?
Comments?
Ideas?

Tilmann Haak <haak@dfn-cert.de>

Sven Übelacker <uebelacker@dfn-cert.de>

Torsten Voss <voss@dfn-cert.de>

https://www.dfn-cert.de/