

JMAP extensions for S/ MIME signing and encryption

draft-ietf-jmap-smime-sender-extensions-02
Alexey Melnikov <alexey.melnikov@isode.com>

Summary

- Extra parameters to "Email/set" command (both optionals):
 - "smimeSign": true
 - "smimeEncrypt": true
 - If both "smimeSign" and "smimeEncrypt" are set to true, the message is first signed and then the signed version is encrypted

Recent Changes

- Added `smimeSignOpaque` (boolean) parameter to control how S/MIME signing is done. The default value is “true” (use `application/pkcs7-mime` container). “false” means use of `multipart/signed` media type.
- Added `headerProtect` (boolean) parameter for signalling S/MIME header protection. The default is “true”.

Next steps

- Add support for S/MIME decryption as well?
- Should JMAP server return blobids for decrypted body parts and let clients use Email/parse on them?