JMAP extensions for S/MIME signing and encryption

draft-ietf-jmap-smime-sender-extensions-01
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

Next steps

- Need a way to control how S/MIME signing is done?

  - multipart/signed or application/pkcs7-mime

  - Tentatively: yes, to allow full control over message generation. The default should be "application/pkcs7-mime"

- Possibly add another parameter for signalling S/MIME header protection?

  - Tentatively: yes. Until LAMPS header protection is deployed, clients might need to control it for backward compatibility

- 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?