JMAP extensions for S/MIME signing and encryption

draft-ietf-jmap-smime-sender-extensions-03
Alexey Melnikov <alexey.melnikov@isode.com>
Summary

- Extra parameters to "Email/set" command (both optionals) to control S/MIME signing and/or encryption:
  - "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.
  - smimeSignOpaque (boolean) parameter controls how S/MIME signing is done. The default value is “true” (use application/pkcs7-mime container). “false” means use of multipart/signed media type.
Recent Changes

- Added `smimeHeaderProtect` (boolean) parameter for signalling S/MIME header protection when signing/encrypting. The default is “true”.

- Email/get operation was extended to support `smimeBlobId` property in the `bodyProperties` request parameter.

- Raw decrypted bytes can be used in Email/parse operation to process decrypted message.
Next steps

- Extend Email/query operation to be able to find “all encrypted” or “all non encrypted” messages.

- Can also allow searching for an email address “S/MIME encrypted to”?
  - This might be different to To/Cc/Bcc recipients.