Extensions to ACME for S/MIME

draft-ietf-acme-email-smime-06

Alexey Melnikov, Isode Ltd

Changes in draft-ietf-acme-email-smime-06 since Montreal

- Added Auto-Submitted header field parameter to help identify challenge emails as ACME S/MIME challenges
- Allow Reply-To header field in challenges
- Clarified which header fields should be protected by DKIM
  - More work needed
- Similar change to email response
- Allow localized reply prefixes for compatibility with existing MUAs
- Added requirement to set In-Reply-To header field in responses
- Updated response payload to include PEM like wrapping
- Allow responses to be multipart/alternative or text/plain media types
- Added initial Security Considerations

Questions raised

- DKIM signing need some changes to disallow extra insertion of header fields into challenge or response messages.
- Security Considerations need improvement.

Next steps

WGLC and ask more feedback on email and S/MIME related mailing lists (LAMPS WG and ietf-smtp)

Background slides

S/MIME

- Goal: be able to get a certificate associated with an email address, which is suitable for S/MIME signing and/or encrypting
- Need a new Identifier Type (email address) and email specific challenge type
- Need some kind of proof of control over the email address: so some kind of challenge (email message sent to the email address) and response (reply email using a more or less standard email client), similar to what happens when subscribing to a mailing list?
  - If an attacker can control DNS, it can reroute email. Assuming that an email owner doesn't control DNS seem to be acceptable risk.

Thank You

- Comments? Questions? Offers to help out with this work? Hackathon?
- Talk to me offline or email me at alexey.melnikov@isode.com