Extensions to ACME for S/MIME

draft-ietf-acme-email-smime-05

Alexey Melnikov, Isode Ltd

Changes in draft-ietf-acme-email-smime-05 since Bangkok

- Tighter definition of how email challenge message looks:
    - Allow FWS (folding white space) instead of a single space
        - They are semantically equivalent in email
        - Implementations can’t expect single space to be preserved on transfer
    - Support for encoded words (RFC 2231) using charset UTF-8 is now required
        - Together with line folding, they are used for “long” subject lines
        - Some libraries/implementations will automatically apply encoded words, can’t be controlled
- Similar change to email response
- Require DKIM or S/MIME signing of challenges

Questions raised

- Allow other Subject prefixes other than “Re: “
  - I would rather not, as I only know of old versions of Outlook that use language specific prefixes on the wire
  - Any other client doing this?
- Use PEM-like encoding for challenges/responses?
  - I prefer to use a new MIME type, it is easier to invoke external programs for them. This can even be text/acme MIME type.
  - For programs that can handle ACME challenge automatically, a new MIME type versa PEM-like encoding are almost the same amount of effort

Open issues in draft-ietf-acme-email-smime-05

- No fancy text/html or multipart/alternative for challenge and response messages?
  - Probably not text/html. Multipart/alternative is more reasonable (clients can display nice HTML if capable), but adds implementation complexity. Multipart/mixed can include a special media type attachment that can be used to invoke and external program on some platforms.
- ~~How to validate email challenges sent by CA?~~
  - ~~S/MIME signed? DKIM signed with valid SPF & DMARC?~~
- Similarly: how to very email responses? DKIM/SPF/ DMARC?

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