Extensions to ACME for email (TLS, S/MIME)

draft-ietf-acme-email-tls-00
draft-ietf-acme-email-smime-00

Alexey Melnikov, Isode Ltd

Email services running over TLS

- Goal: being able to get a certificate for SMTP submission, IMAP, etc servers
- According to **RFC 7817,** such certificates either contain **dNSName** or **srvName** in certificate's subjectAltName
  - srvName is nice, because it can limit protocols a certificate can apply to.
- Requirement: avoid the need to run an HTTP server on the same hostname in order to get an ACME certificate
  - One can just use base ACME protocol to get a certificate with dnsName and reuse it for email. ***But key usage in the certificate can be wrong.***

Email services running over TLS - proposals

- Options 1:
  - Extend DNS verifier to specify protocol and possibly port number
    - E.g. _993._imaps._acme-challenge.example.com
    - Pros: sysadmins running email services usually have DNS control over the corresponding domain (e.g. to set MX, SRV, DKIM and DMARC TXT records)
    - Cons: in some domains people controlling DNS and people controlling email services are different groups of people

Email services running over TLS - proposals

- Option 2:
  - Define extensions to SMTP/IMAP to advertise proof of control over the corresponding SMTP/IMAP service
    - Pros: no need to change/add DNS records
    - Cons: either need to restart SMTP/IMAP service to publish “proof of control over domain” or might need to redesign the server to be able to publish such proof without restarting

Email services running over TLS - proposals

- Option 3:
  - Use of Service Name Indication (SNI) TLS extension with special certificates that convey “proof of control over domain”
    - Pros: no need to change SMTP/IMAP implementations, no need to change DNS
    - Cons: need to have TLS stack (or server logic using the TLS stack) that supports ALPN and special ACME certificates.
    - Cons: might need to restart SMTP/IMAP service or redesign it to allow publishing new certifixates without service restart

Email services running over TLS - proposals

- Do we need to choose 1 (or at least less than 3) option?

- Other changes:
- JWS object is extended to include “service” (e.g. “smtp”, “imaps”) and “port” attributes

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.
  - Is being able to just read email a sufficient proof of control?

Thank You

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