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

draft-ietf-acme-email-tls-02
draft-ietf-acme-email-smime-01

Alexey Melnikov, Isode Ltd
Changes in draft-ietf-acme-email-tls-02 since Prague

• Removed TLS SNI challenge, the other 2 (DNS and SMTP/IMAP capabilities) remain
• Added a reference to RFC 7817, which defines what email clients are looking for/CAs should include in email certificates for TLS server identity verification to work
• The “port” JWS header parameter is now not required (“service” still is)
• Fixed some typos, added missing references.
• Expanded the list of open issues.
Open issues in draft-ietf-acme-email-tls-02

• Should “service” (e.g. “smtp”, “imaps”) and “port” values be included in ACME challenge hashes?
  • I think yes. Might need some help from ACME specialists.

• Should the same ACME certificate be allowed to cover both TLS and non TLS ports?
  • Probably not, as a single challenge can only include 1 service name and service names for the 2 are different (e.g. “imap” for port 143 and “imaps” for port 993).

• Support LMTP (RFC 2033)
  • Probably yes, but need to register “lmtp” as a service name first.
Next step

• Have at least a couple of reviews? (Richard?)
• Anybody interested in implementing?
Changes in draft-ietf-acme-email-smime-01 since Prague

- Added support for RFC 6531 (internationalized email addresses)
  - LAMPS WG is updating X.509 certificates and we need a new identifier type anyway
- Clarified that both challenge and responses emails are in plain/text
  - This provides highest degree of interoperability in email world and is also friendly to use of external tools and use of cut & paste for ACME challenges
Open issues in draft-ietf-acme-email-smime-01

- 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
- The document assumes that we need to prove ability to send messages as an email address, not just read email.
Background slides
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.
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
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