Security CallFlows

draft-ietf-sip-sec-flows-01

Robert Sparks

Status

- Automating creation of examples
  - Mostly done, but non-trivial detail work remains
- Addition of test cases
- Attempt to capture certificate matching rules

Matching Certificates

- Rules aren’t adequately captured
- Identity tries to clarify
- This draft tries to capture those matching rules for the general SIP with S/MIME and SIP with TLS cases
  - Remember that this draft is not normative

Matching Certificates

- For S/MIME the peer's URI must appear in the subjectAltName of the peer's certificate as a uniformResourceIdentifier field.
- For TLS the peer's hostname (as fed into 3263 for resolution for locating the peer) must appear as
  - an exact match in a dNSName entry in the subjectAltName if there are any dNSNames in the subjectAltName. (Wildcard matching is not allowed against these dNSName entries)
  - the most specific CommonName in the Subject field if there are no dNSName entries in the subjectAltName at all (which is not the same as there being no matching dNSName entries). This match can be either exact, or against an entry that uses the wildcard matching character '*'