Domain Certificates in SIP

Vijay K. Gurbani, Scott Lawrence, and Alan Jeffrey

draft-gurbani-sip-domain-certs-03

67th IETF (November 5-10, 2006)

San Diego, CA (USA)

Problem

- What identities appear in a X.509 certificate for SIP clients and servers?
- The HTTP model: one identity (www.example.com), all servers in a farm share this certificate.
- In SIP, this works fine for a request with a high-level URI (sips:alice@example.com), but …
- Proxies R-R with their FQDN name (sips:downtown.example.com), so on a subsequent contact, example.com != downtown.example.com.
- The system creating a TLS connection may be authoritative for its SIP Domain as a sender without being in the set of proxies resolved by NAPTR/SRV for that domain (outbound vs. inbound proxies).

Solution

- Two issues to be solved:
  - An authoritative way to express the purpose of the certificate: easy for implementers to code against, and CAs to enforce.
  - Identify the host presenting the certificate.

- Draft proposes inserting two identities in the certificate:
  - sip:example.com => The system is authoritative for the SIP domain that is named.
  - dns:downtown.example.com => The system is authoritative for the name used as the transport address.

WG List Discussion

- Consensus on
  - having multiple identities in the SAN of the certificate (EKR proposed a list of rules that are appropriate; see http://www1.ietf.org/mail-archive/web/sip/current/msg17028.html)
  - Do not break the names into sip and dns schemes.
  - Use OIDs for enunciating the purpose of the certificate
    - The use of ‘sip:’ URI
    - The addition of an extendedKeyUsage OID (will be in next version of the draft)

Next Steps

- WG interest in pursuing this?
- WG item?