Certificate Directory for SIP

Cullen Jennings
fluffy@cisco.com

SIP Security & SMIME

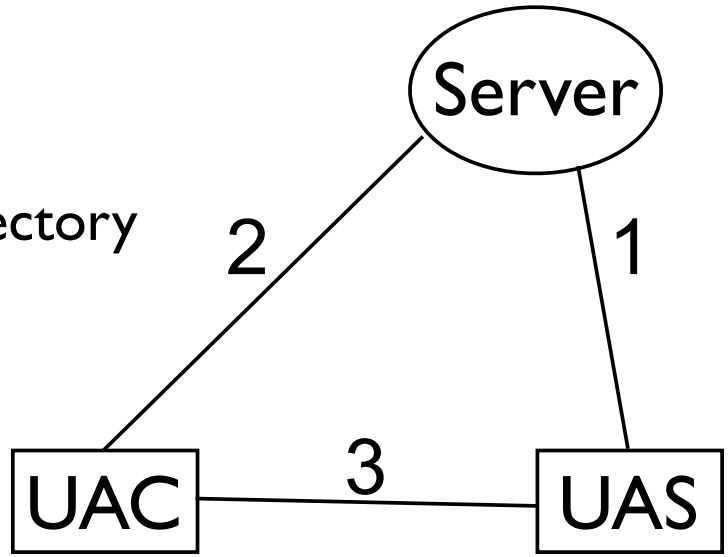
- SIP Security depends on S/MIME with user certificates
  - Encryption of SDP (and keys for SRTP)
  - Refer
  - Identity
  - Request History
  - End to Middle? Middle to End?
- This requires Certificates in the UA's

Certificates

- Traditional "PKI" certs (like Verisign)
  - Problem: Enrollment difficulty and yearly fee to CA
- Private CA certs
  - Problem: Only work if all callers have this CA as a trust anchor.
- Self signed certs
  - Problem: Need a directory to store certs and vouch for them

Certificate Directory

- Way for UAC to locate the directory
  - use domain from AOR
- Way for the UAC to authenticate the directory
  - use traditional PKI
- Way to fetch certs
  - HTTPS, LDAPS, other
-
- Way to store certs
  - HTTPS, LDAPS, Sacred
- Way for directory to authenticate the UAS
  - reuse SIP credential (Digest shared secret)
- Way for the UAC to authenticate the directory
  - use traditional PKI



Proposal

- Wrote a draft using the HTTPS options
  - draft-jennings-sipping-certs-01
  - 00 version done before last IETF
  - Several security people have looked at it
    - They believe it works and can be reasonably secure
- Provides certificates with minimal cost
  - Introduces an extra TLS connection setup to calls with no cached certificate
  - Requires each domain to run an e-commerce style web server
  - Is only as trustable as the server is trustable
- **Does the WG want to solve this problem?**