Domain-certs
(draft-gurbani-sip-domain-certs-01)

66th IETF, July 2006

Montreal, Canada

Vijay K. Gurbani, Alan Jeffrey

Identities in Certificates

- The Web model:
  - *f*(URI X) => C
  - URI X == C?
- More concretely:
  - If https://www.example.com elicits a certificate with “DNS:www.example.com”, authentication is successful.
- This works for SIP, too: sips:alice@example.com elicits a certificate of “DNS:example.com”.

Identities in Certificates

- Problem with corner cases
  - Requests that contain other than a domainname in the R-URI/Route.

  INVITE sips:alice@downtown.atlanta.com SIP/2.0
- Server certificate contains “DNS:atlanta.com”.
  - Does “downtown.atlanta.com” == “atlanta.com”?
    - downtown may be a subordinate domain.
    - Or it may be a host in the atlanta.com domain.
- Also:

  INVITE sips:alice@atlanta.com SIP/2.0

  Route: <sips:downtown.atlanta.com;lr>

Mutual Authentication

- Client authenticates server ➔ OK.
- Server authenticates client ➔ How?

```
INVITE sips:alice@atlanta.com SIP/2.0
From: <sips:bob@biloxy.com>;tag=o981iU
Via: SIP/2.0/TLS sip1.example.com;branch=…
```

- Client certificate contains “DNS:example.com”.
  - Match what: From? R-R? Via sent-by?

Multiple Identities Certificate?

- Having multiple identities in certificates appear to solve some of the corner cases:
  - DNS:example.com
  - DNS:sip1.example.com
- Why is this not preferred?

Odds and Ends

- Other issues in the draft:
  - Proxy farms (depends on the resolution of how identities are represented).
  - Virtual servers.