X.509 Authentication in the RIPE Database

Shane Kerr, RIPE NCC

Motivation for X.509

- *Improved Secure Communication* effort
  - Easier/more secure LIR-RIPE NCC communication
  - Single authentication token
  - Leverage existing technology and standards
- Use these client-side certificates with DB
- Web updates with strong authentication

Background & Status

- July 2003 proposal sent
- September 2003, RIPE 46, revised proposal
  - Basically this proposal, presented informally
- January 2004, RIPE 47, final (hopefully) proposal
  - No changes, but documents implementation
  - S/MIME survey also published (presentation follows)
- February 2004 – implementation (hopefully)

Details

- Changes key-cert class to represent X.509 certs
- Changes “auth:” attribute
- Add S/MIME updates
- Add client-side authentication for SSL updates

Changes to key-cert class

- “key-cert:” additional format X509-nnn
- “method:” X509
- “owner:” is Distinguished Name (DN)
- “fingerpr:” is the MD5 fingerprint
  - Also becomes a lookup key
- “certif:” is the ASCII representation

“key-cert:” attribute

- X509-nnn
- Generated by the database
- Like “nic-hdl:”, *except…*
  - Guaranteed unique
  - No DoS/hijacking issues
  - No re-use
  - No choice in name – only meaningful as a database key

key-cert Example

```
key-cert:  X509-42
method:    X509
owner:     /C=NL/O=RIPE NCC/OU=Members/CN=eu.ripe-ncc.shane/Email=shane@r...
fingerpr:  D5:92:29:08:F8:AB:75:5F:42:F5:A8:5F:A3:8D:08:2E
certif:    -----BEGIN CERTIFICATE-----
certif:    MIID/DCCA2WgAwIBAgICAIQwDQYJKoZIhvcNAQEEBQAwcTELMAkGA1UEBhMCRVUx
certif:    EDAOBgNVBAgTB0hvbGxhbmQxEDAOBgNVBAoTB25jY0RFTU8xHTAbBgNVBAMTFFNv
  .
  .
  .
certif:    hZNmF5c/d0gauqvL+egb+3V+Zg+sJTzHMVKQLF1ybWgJjU75Pi+mO7BG0zsQ13p
certif:    YxuZCR2W15nwt7zLiHtmfw==
certif:    -----END CERTIFICATE-----
remarks:   Sample Key Certificate
notify:    ripe-dbm@ripe.net
mnt-by:    RIPE-DBM-MNT
changed:   ripe-dbm@ripe.net 20040101
source:    RIPE
```

“auth:” attribute change

- Current forms:
  - NONE
  - CRYPT-PW
  - MD5-PW
  - PGPKEY-xxxxxxxx
- New form:
  - X509-nnn
- Example:

```
auth: X509-17   # what could be simpler?
```

Update Changes

- S/MIME
  - Signing only
  - Can combine fully with other methods (password/PGP)
- Client-side SSL
  - Web Updates
  - Sync Updates