X.509 Support for the Hostmaster Robot

Shane Kerr, RIPE NCC

Outline

- Secure Communications with LIRs (PKI Project)
- Current Status and Next Steps
- X.509 and the Hostmaster Robot
- Questions

Secure Communications with LIRs a.k.a. the PKI Project

- Goals:
  - Security
  - Single method for all communications
  - Convenient and easy to use
- Documented in RIPE NCC activity plans
- “Formal” proposal to community in April 2003
  - Uses X.509 technology
  - Phased implementation

X.509

- Maturing technology
- Single authentication token (certificate) for:
  - Web-based interaction (client-side SSL)
  - E-mail based interaction (S/MIME)
- Only for LIR ↔ RIPE NCC communication
  - No authentication to 3rd parties
  - Simplifies design, procedures
  - Eliminates various security and reliability issues

Outline

- ✓ Secure Communications with LIRs (PKI Project)
- Current Status and Next Steps
- X.509 and the Hostmaster Robot
- Questions

Current Status

- LIR Portal
  - Users can obtain and revoke a certificate
  - Users can log in to the portal
- RIPE Database
  - Final proposal has community consensus
  - Implementation ready to deploy
  - Similar to existing PGP security in the database

Next Steps

- Time to secure the e-mail to hostmaster@ripe.net
- Non-repudiation
  - Insure that requests come from authorised people
  - Guarantee that replies come from the RIPE NCC
- Confidentiality
  - Business plans
  - Purchase orders

Outline

- ✓ Secure Communications with LIRs (PKI Project)
- ✓ Current Status and Next Steps
- X.509 and the Hostmaster Robot
- Questions

X.509 and the Hostmaster Robot

- Non-repudiation first (signing)
  - More straightforward
- Confidentiality second (encryption)
  - Tricky
  - Details of approach depend on user needs
  - *Your input necessary!*

Signing

- LIR can configure the details
  - Users can specify how they want to send & receive
  - Administrator can override user preferences
- LIR e-mail to RIPE NCC
  - Default is always: current behaviour
  - If desired, S/MIME can be required
  - Final failure mode is always a human
- RIPE NCC e-mail to LIR(s)
  - Default is always: current behaviour
  - If desired, S/MIME can be used
  - In mixed cases, both PGP and S/MIME will be used

Outline

- ✓ Secure Communications with LIRs (PKI Project)
- ✓ Current Status and Next Steps
- ✓ X.509 and the Hostmaster Robot
- Questions

Questions

- Do members' security concerns in communication with the RIPE NCC require encryption?
  - For all mailboxes?
  - For inbound and outgoing mails?
- What is the appropriate security / service balance?
  - Expired certificates when encryption desired
  - Lost / compromised certificate recovery
- How complex can the system be?
  - Mails to multiple recipients (e.g. mergers and takeovers)

Future Feedback

Please see full text on-line, and reply with any feedback:

http://www.ripe.net/ripe/mail-archives/ncc-services-wg/2004/msg00016.html

Contact e-mail: pki-suggestions@ripe.net