PKI deployment at the RIPE NCC

Improved Secure Communication System

Andrei Robachevsky, andrei@ripe.net
RIPE NCC

What has been done

- Motivation, objectives and the outline of the plan
  - Presentation at the RIPE 43
    http://www.ripe.net/ripe/meetings/archive/ripe-44/presentations/ripe44-plenary-secure/
  - Draft Document
    http://www.ripe.net/ripe/draft-documents/pki-20030429.html
- PKI components are developed and deployed
  - RA – LIR Portal (https://lirportal.ripe.net/lirportal/activation/activation_request.html)
  - CS, CR, PMS – internal
- Services available
  - LIR Portal
    - Allocation editor, Request forms

In Progress

- X.509 authentication in the RIPE DB
  - A new auth method (+ NONE, CRYPT-PW, MD5-PW, PGPKEY)
  - Transparent authentication via webupdates interface
  - S/MIME support
    - Research is in progress on compatibility and reality check
  - Initial proposal got interesting feedback
    - Key-cert object, support for third party certificates
- Integration with the LIR Portal
  - A “mntner manager” for creation/modification
  - Single sign-on

Future plans

- Correspondence with the RIPE NCC
  - Signing and encrypting using X.509 certs
- Authentication, non-repudiation, confidentiality
- Issues
  - S/MIME compatibility
    - Research is ongoing
  - PGP
    - Discontinue signing outgoing messages ?
    - Sign and encrypt at user's choice ?