APNIC Certification Authority Overview

APRICOT 2005
Kyoto, 21 – 25 Feb 2005

Sanjaya, Project Manager, APNIC Secretariat

Motivation

- In response to
  - Membership concern for greater security
    - Confidential information exchange with APNIC
    - Is my database transaction secure?
    - Whose prefixes do you accept?
  - Internet community interest in security, PKI, digital certificates
    - e.g. rps-auth, s-bgp
    - IETF working group: PKIX

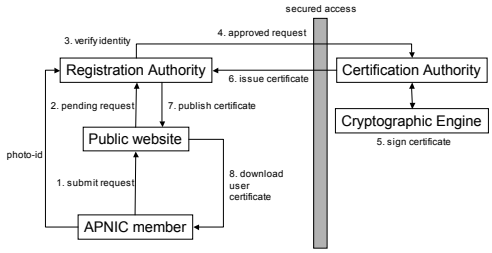
Scope

- Establish a trusted environment within APNIC community by operating a Certification Authority
  - Certificate issued to APNIC member
    - Corresponds to *Membership* of APNIC
- A test bed for new internet security technologies and applications

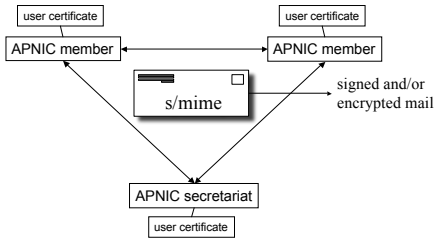
Objective

- Provide uniform mechanism for all security needs:
  - Encryption and signature of email with APNIC
  - Authentication of access to APNIC web site
  - Secure maintainer mechanism for APNIC database
  - Authorisation mechanism for Internet resources
    - Assertion of resource delegation
      - » IPv4
      - » IPv6
      - » ASN

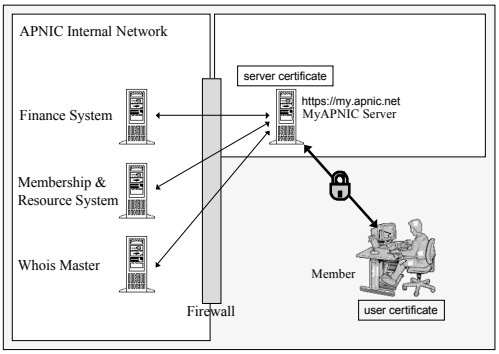
APNIC CA configuration



Secured e-mail

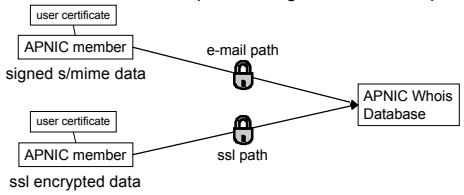


Secured web portal - MyAPNIC



Secured database update

- Available 2Q 2005
  - Allows secured update using automated script



Assertion of resource delegation

- Subject to membership approval
- Available 4Q 2005
- Implementation of RFC3779
  - New certificate format

Base certificate:
- dn: cn=John Sing o=EXAMPLENET-AP
- etc.

Extension:
- IPv4: 202.100.0.0 – 202.100.15.255
- IPv6: 2001:400::/32
- ASN: 23509

For more information

- APNIC public website
  - http://www.apnic.net
- Certificate request
  - https://www.apnic.net/ca
- MyAPNIC
  - https://my.apnic.net