APNIC RPKI Implementation Status

ggm@apnic.net

Our Lead Coder

APNIC RPKI Implementation Status

- The operational model
- The user model
- Implementation language
- The RPKI features implemented
- The status

The operational model

- APNIC Operates Two distinct RPKI engines
  - "APNIC the RPKI" –APNIC certifies what it has done facing its direct relationships
  - 'Hosted Clients' –What APNIC does on behalf of its resource holders, but they make it happen
- Communicate over up-down internally
  - Shared bPKI but virtualized channel one per member
- Separated back-end signer via XML/REST
  - HSM backed

The user model

- We’re not in the s/w business.
  - We have shared code (AfriNIC) but its not our core business
  - This service is internally hosted, managed, maintained
- We expect most (by number) APNIC direct members to use the hosted solution for the forseeable future

Implementation language

- Perl 5
- OpenSSL engine logic to LunaSA
- Use Rob Austein OpenSSL RFC3779 code
  - "it works"
- Some issues with parallel access to HSM
- REST/XML used internally
  - https secured channels between communicating parts
- Considering re-implementation costs of signer function eg into EJBCA/Java, use of middleware

The RPKI features implemented

- UP

The RPKI features implemented

- UP
- Down

The RPKI features implemented

- UP
- Down
- A bit of sideways

The RPKI features implemented

- UP
- Down
- A bit of sideways
  - We push content to repository, but we don't have publication protocol right now

The RPKI features implemented

- UP
- Down
- A bit of sideways
  - We push content to repository, but we don't have publication protocol right now
  - Hence many stale objects in repository (sorry)

The RPKI features implemented

- UP
- Down
- A bit of sideways
  - We push content to repository, but we don't have publication protocol right now
  - Hence many stale objects in repository (sorry)
- Hosted portal via MyAPNIC provides end-services to make/manage ROA, signed objects

The RPKI features implemented

- UP
- Down
- A bit of sideways
  - We push content to repository, but we don't have publication protocol right now
  - Hence many stale objects in repository (sorry)
- Hosted portal via MyAPNIC provides end-services to make/manage ROA, signed objects
- We don't do validation/client side tools

The status

The status

- Its live.
- We have around 379 certs (hacktrn/rsynic) and 22 ROA objects (that are not stale)
- APNIC the RPKI is fully HSM backed
- We're still doing soft key on members but will migrate once we fix some HSM scaling issues
- Offline TA made on a SafeNet CA4
  - Not TAL, but close
- We've done reasonably complete interop with ISC code, and have a semi-permanent testbed live hosted by the ~~DHS NSAPSG~~ Randy's VM

The Bugs

- BPKI needs work
  - Need to accept intermediate CA, and validate EE used on the wire. Need CRL.
  - BPKI induction process needs minor nits work
    - We're pretty happy with the XML used for exchange
  - Once this is done, we think we can discuss up-down as a service more rationally
- We need work to sweep our repository
- We need to confirm our multiple-parent and RPKI classes behaviour
  - Required for global trust anchor

Coming Soon

- We have a long-lifetime ‘whole of APNIC’ tree signed internally
- Every resource holder, CA/EE and manifest
- Long life CRL so won’t require re-runs
- Intend publishing as a stable testbed resource reflecting the status quo as of 1Q2011 to aide relying party coders
- It was slow to make. We need to work on parallelism in our system
  - Hence the concern over the HSM parallelism bug


THUNDERBIRDS


THUNDERBIRDS


THUNDERBIRDS
FA


THUNDERBIRDS
FAB