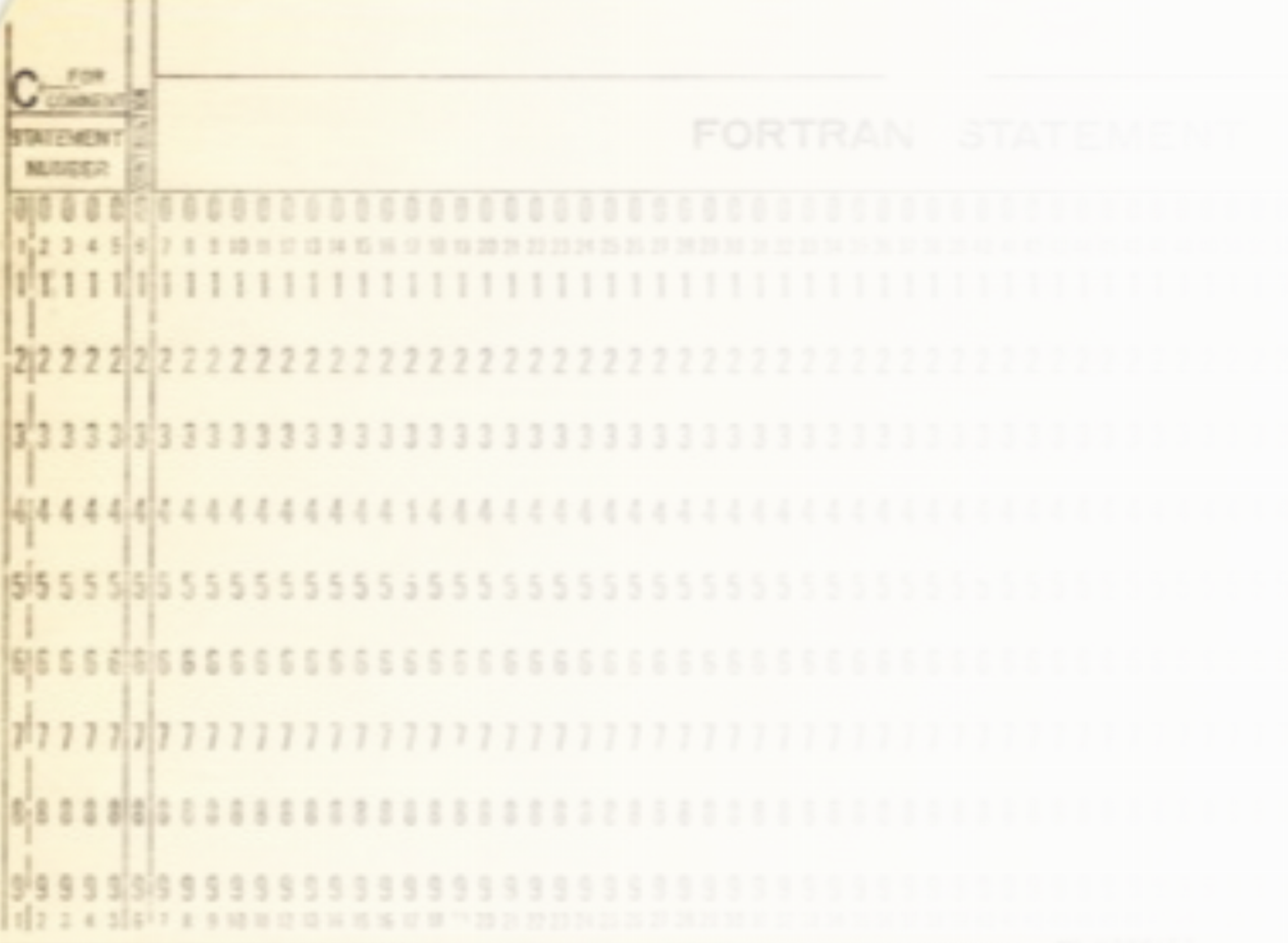

C FOR COMMENT
STATEMENT NUMBER
CONTINUATION
FORTRAN STATEMENT

APNIC RPKI Report

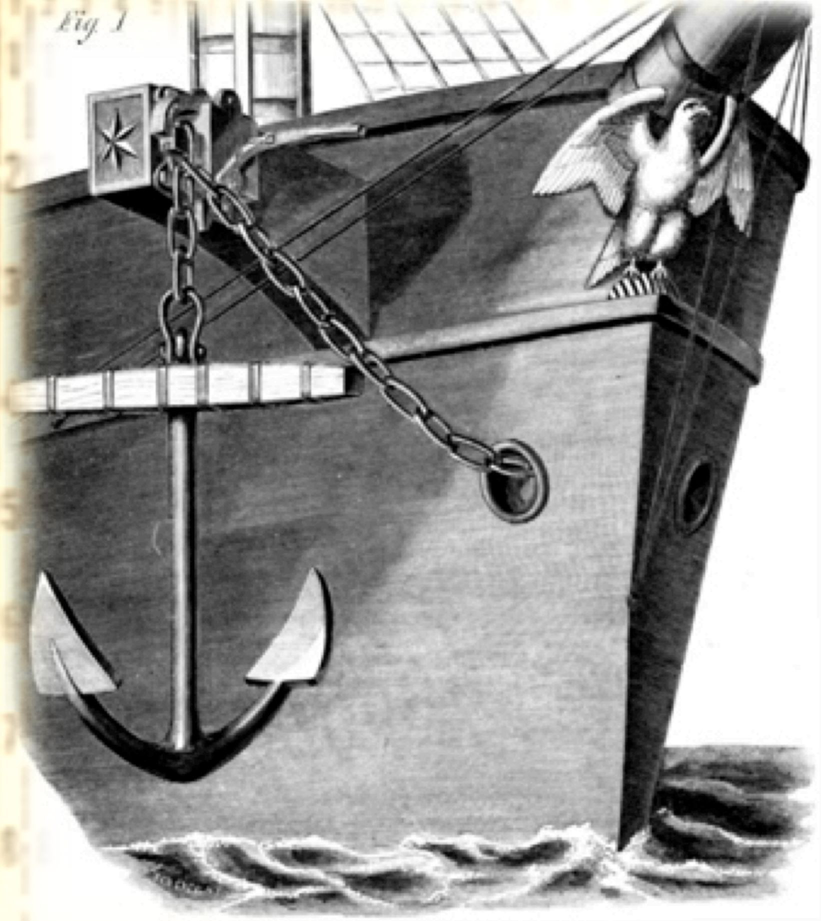
George Michaelson

APNIC RPKI – Current Activities

- The RPKI TA Framework
- APNIC’s TA Changes
- Provisioning Protocol Services

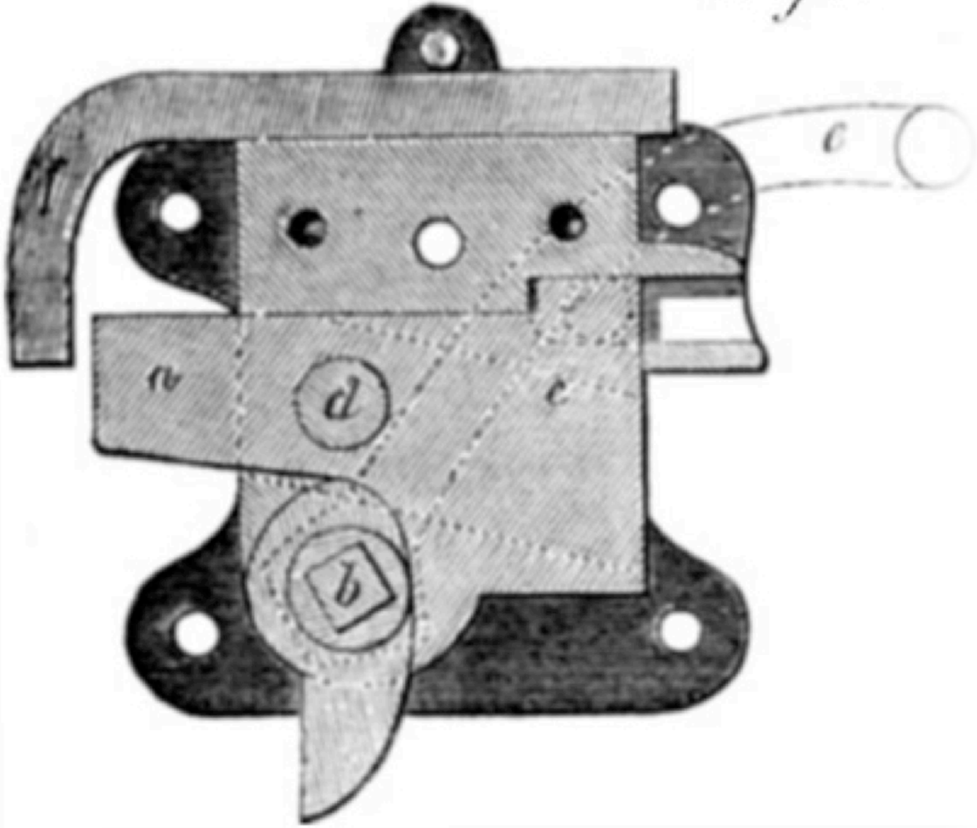
The RPKI TA Framework

Fig. 1



BAYLIES'S ANCHOR TRIPPER.

Fig. 2



The RPKI TA Framework

- Managing TAs is an issue of concern in the RPKI because the integrity of the assertions will be ‘tested’ by relying parties against the TAs they hold.
- At present there is no single TA covering the entire span of the IP address space.
  - Today we use a collection of TAs, where each TA encompasses a subset of the address space under separate registry management.
- Each Regional Internet Registry publishes its own public key as a ‘putative’ TA for relying parties to use.

The RPKI TA Framework

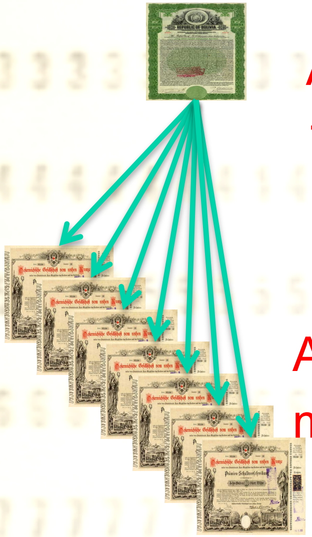
- TA management is not directly defined by the RPKI standards, except in respect of the TA Locator or ‘TAL’
  - Mechanism to fetch public key of TA, and URL to fetch it.
  - Relying parties can obtain the root RPKI certificate, and then anchor validation chains of RPKI certificates.
- A relying party can use multiple TAs, and these can encompass overlapping ranges of Internet Number Resources,
  - because the validation process is defined as finding **any** TA which can validate the resources in the PKI
  - not a **specific** TA.

APNIC's TA Changes

Der Riesen-Anker (Gewicht 300 Centner
Nordische-Hafen-Ausstellung-Kiel 19

APNIC's TA Changes

- When APNIC started deploying RPKI, it adopted a simple model of anchoring its resources in a single TA.



APNIC Trust Anchor Certificate
1/8, 14/8, 36/8,...

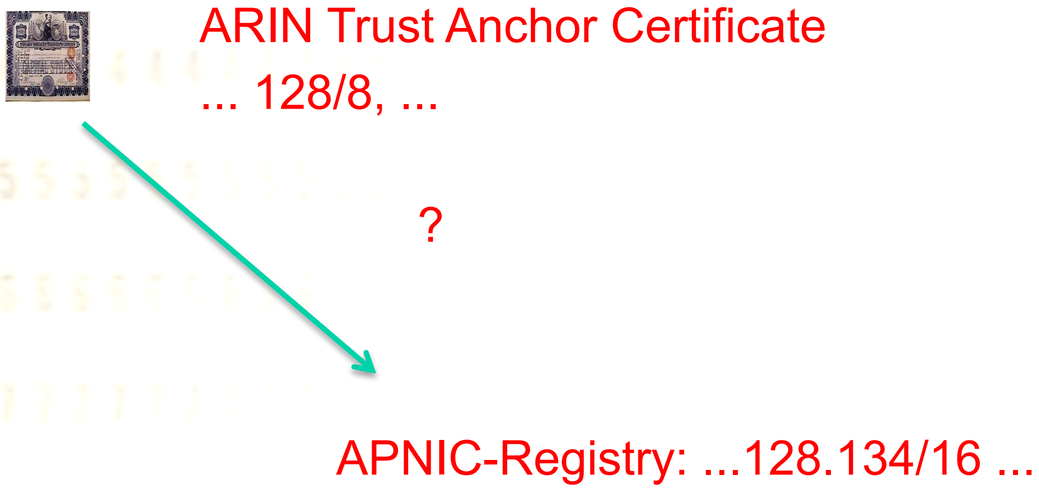
APNIC-Issued Certificates for resource-holding members

APNIC's TA Changes

- When APNIC started deploying RPKI, it adopted a simple model of anchoring its resources in a single TA.
  - This was easy to deploy
  - reflected our understanding at the time
    - internet number resources we had administrative management authority over within APNIC's registry,
    - as distinct from the other RIR registries that provide number resource management.

APNIC's TA Changes

- As the RPKI project has progressed, other RIR are now publishing their own TA, and these TAs include resources that are contained in the APNIC registry.



ARIN Trust Anchor Certificate
... 128/8, ...

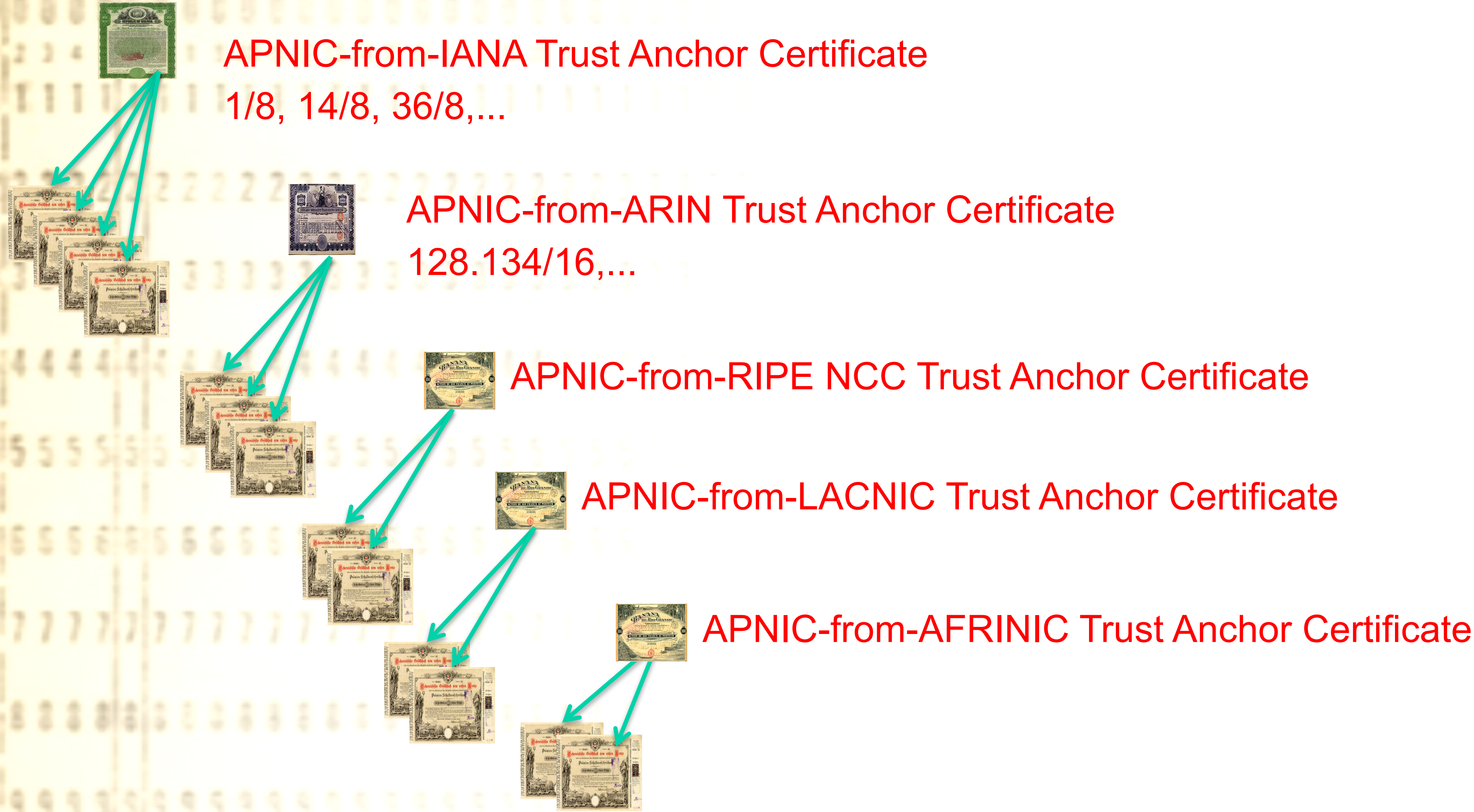
?

APNIC-Registry: ...128.134/16 ...

APNIC's TA Changes

- Re-align our issued certificates to accurately reflect the "provenance " of the resources that are held in our registry.
  - E.G. if a resource in APNIC's registry is a fragment of a larger block that is held in the RIPE NCC's registry, then we would like to use a certificate structure that reflects this.
- Structure APNIC's RPKI certificate collection, and the associated TA material
  - Reflect the hierarchy of registry responsibility for internet number resource management.

APNIC's TA Changes



APNIC-from-IANA Trust Anchor Certificate

1/8, 14/8, 36/8,...

APNIC-from-ARIN Trust Anchor Certificate

128.134/16,...

APNIC-from-RIPE NCC Trust Anchor Certificate

APNIC-from-LACNIC Trust Anchor Certificate

APNIC-from-AFRINIC Trust Anchor Certificate

APNIC's TA Changes

- APNIC’s TA are 5 discrete components, reflecting the different ‘inheritance’ paths
  - Resources for which IANA has assigned responsibility to APNIC.
    - Number blocks described in the IANA number registries as being assigned to APNIC, such as 42.0.0.0/8 and 2400::/12
  - Resources managed by APNIC, transferred as a fragment of a larger number block, that is administered by another RIR.

APNIC's TA Changes

- This *inter-RIR registry arrangement* is typically the result of a relocation of administrative control from one RIR region to another
  - E.G. when a multinational entity decides to move Internet Number resource management from Europe to its Asian office
  - may arise from an inter-RIR address transfer.
- Split TA maintains a direct relationship between the RPKI certificate structure and the specific path of registry responsibility that APNIC has over those resources through another RIR

APNIC's TA Changes

- By converting to this split TAL model **now**:
  - APNIC avoids any future need to re-issue operating certificates, and the associated resources held by members in future.
  - Given that we have few products published now, but intend promoting RPKI strongly through 2013, we have avoided a future migration for all RPKI certified members.

APNIC's TA Changes

- Other RIRs have taken a different approach and have opted to publish all resources they hold under the hierarchy of a single "root" certificate, which is, in effect, their TA.
- Right now we are not sure if this represents the preferred option for the community of RPKI relying parties.
  - If there is a desire to further simplify the APNIC TA structure it is possible to generate a single encompassing certificate and publish a single APNIC TA.

APNIC's TA Changes

- We would like to understand the larger story of the overall direction of RPKI trust anchors and the community preference relating to the management of trust anchors across the entire RPKI as a precursor to further changes in this area.

Provisioning Protocol Services

Provisioning Protocol Services

- APNIC has been running a provisioning protocol (the “up/down” protocol) since the inception of our web portal service.
  - The MyAPNIC portal uses provisioning protocol to talk to the APNIC RPKI engine
  - to ensure strict separation between the RPKI products we make, as a registry, and the RPKI products that our members direct us to make.

Provisioning Protocol Services

- However, we hadn’t provided a publicly visible port of this RPKI certificate management protocol to the wider community
  - we didn’t have any mechanism to exchange business PKI information, which is necessary since the messages which flow over provisioning protocol are signed CMS.

Provisioning Protocol Services

- We have written a simple Interface on the MyAPNIC Portal to permit members to upload their business PKI (bPKI)
  - using the RPKI.NET defined XML which encodes the trust chain, behind the certificate which will be used ‘on the wire’ to sign the CMS.

Provisioning Protocol Services

- By incorporating this key material into the APNIC trust set, we can validate
  - that the CMS part of the subsequent protocol exchange is well signed,
  - that the certificate chain over it reflects the currently known authority provided by that member.

Provisioning Protocol Services

- We believe this is a good reflection of community expectations, although its details are not currently defined by any standards or draft-standard.
  - Rob Austein, the developer, has informed us that the XML may well change in 2013 to reflect changes in his model of provisioning new bPKI relationships
  - we intend working to adopt his new model as it is defined.

Provisioning Protocol Services

- APNIC has also identified process complexities in migrating from an existing hosted solution (using MyAPNIC to create RPKI outcomes) to an external (self-hosted) system.
  - Obvious risks where there is both a "live" RPKI space in the MyAPNIC managed service area, and a “live" RPKI space managed entirely by the member.
  - We are designing a User Interface which clearly identifies the transitional stages, and ensures the member is clearly in charge of the transition process at all times.

Comments?