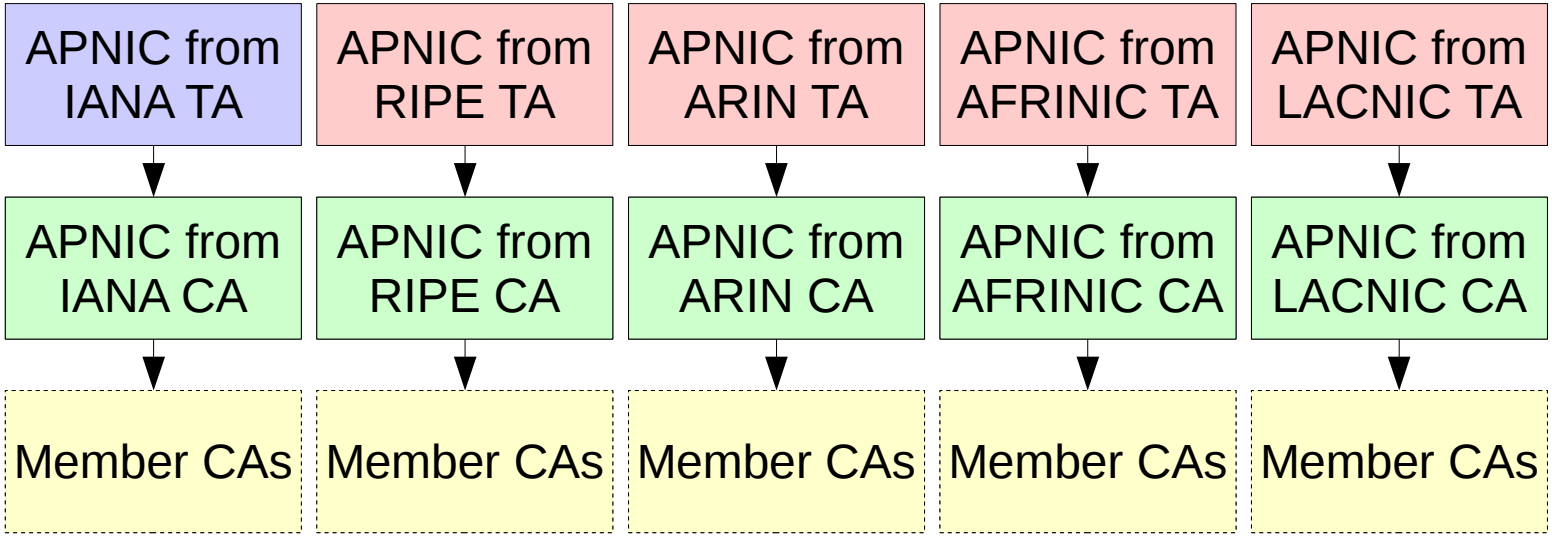
APNIC 44

Transitioning to a single RPKI trust anchor

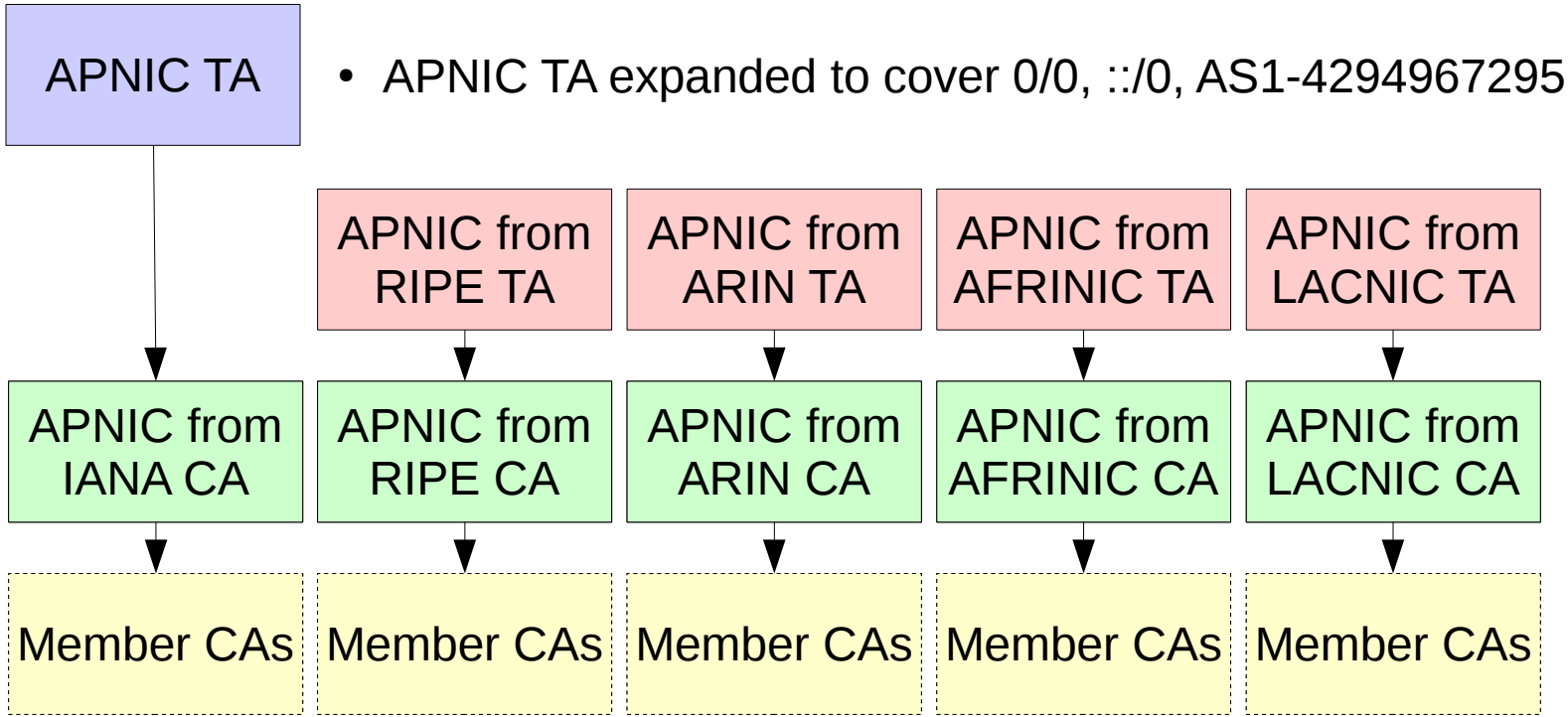
TAICHUNG, TAIWAN
7–14 September 2017

#apnic44

What is the current state?

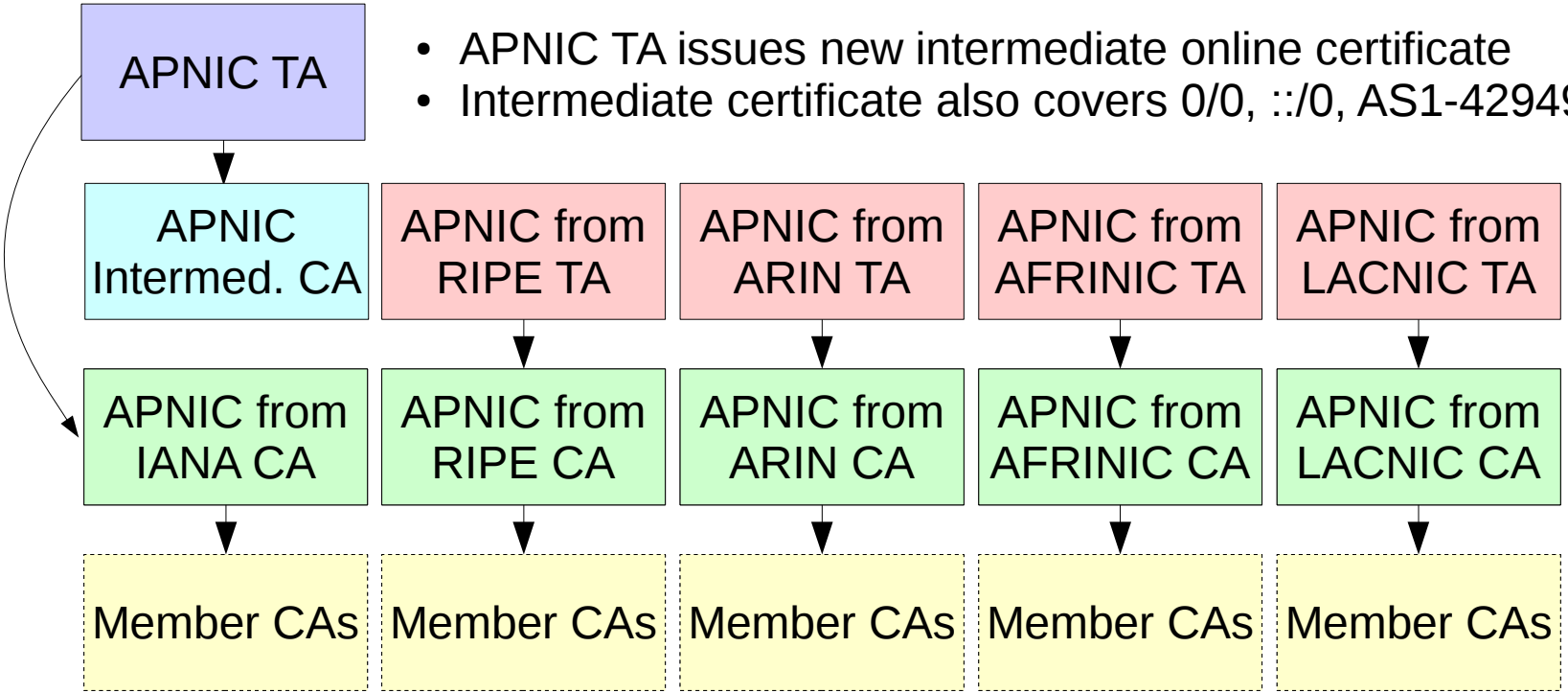


How does the transition happen? (1)



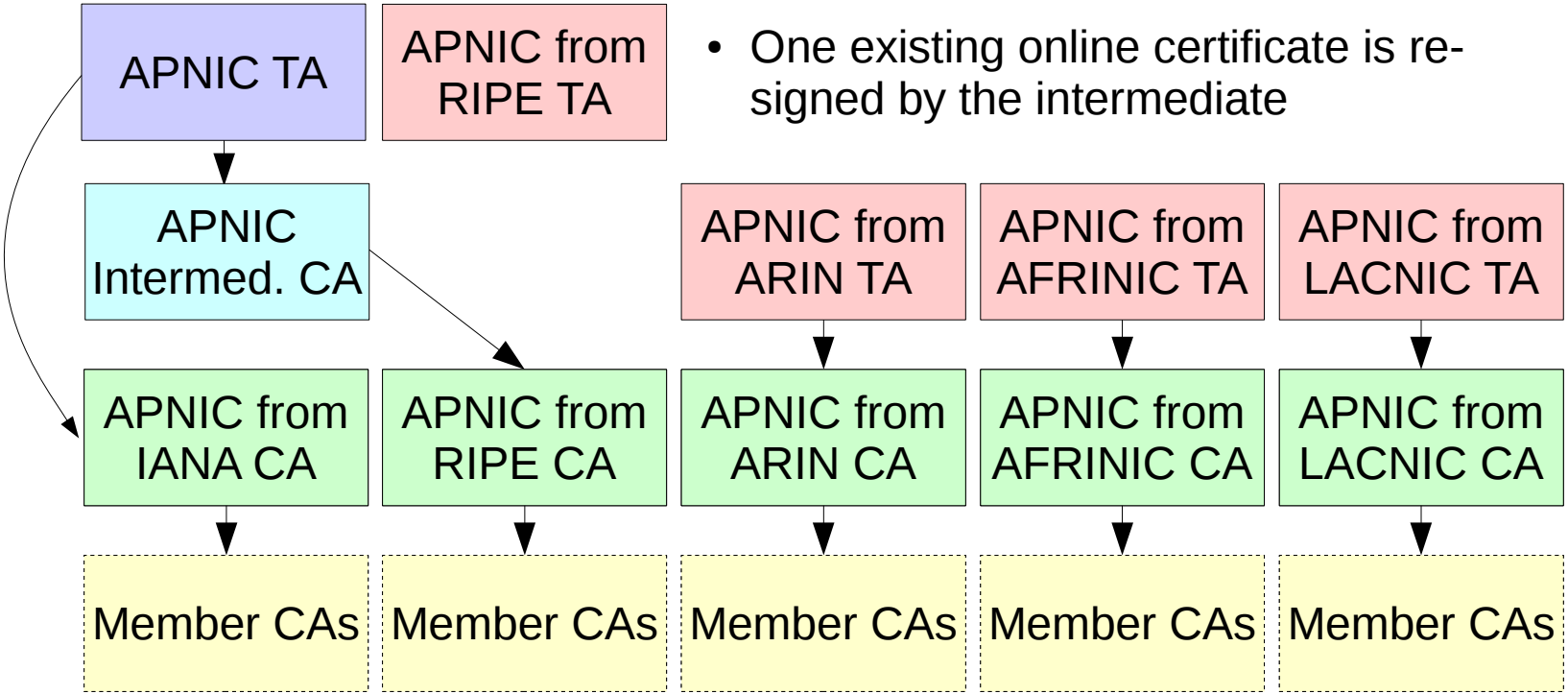
- APNIC TA expanded to cover 0/0, ::/0, AS1-4294967295

How does the transition happen? (2)



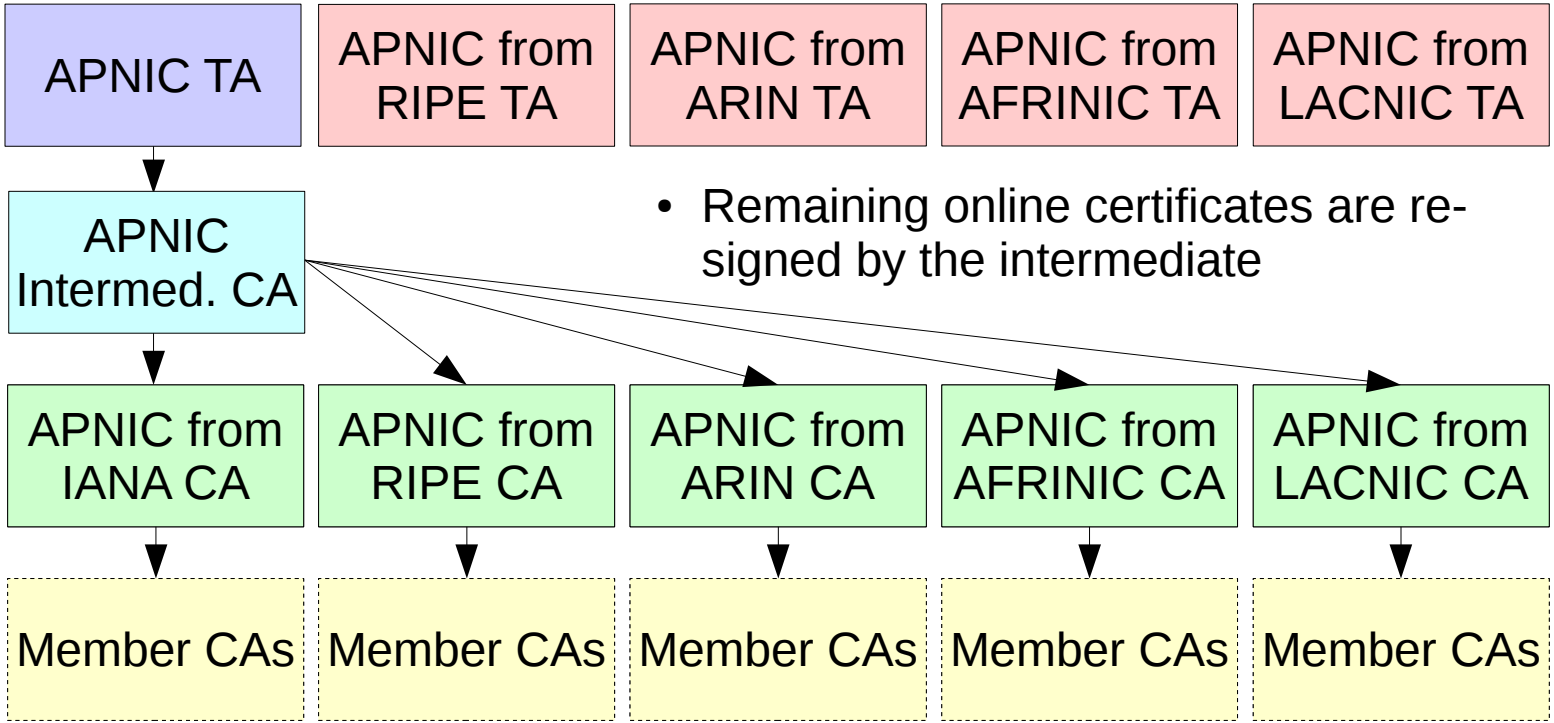
- APNIC TA issues new intermediate online certificate
- Intermediate certificate also covers 0/0, ::/0, AS1-4294967295

How does the transition happen? (3)

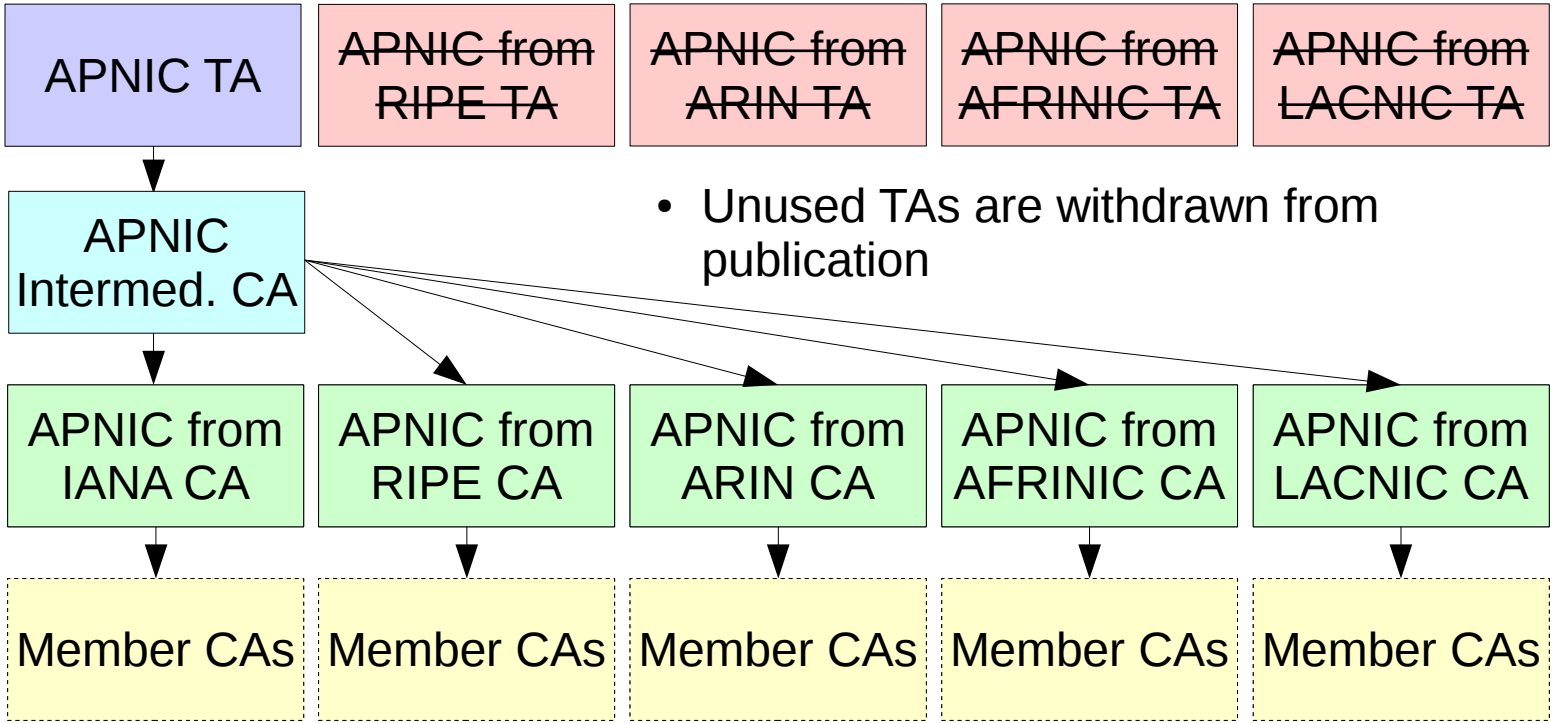


- One existing online certificate is re-signed by the intermediate

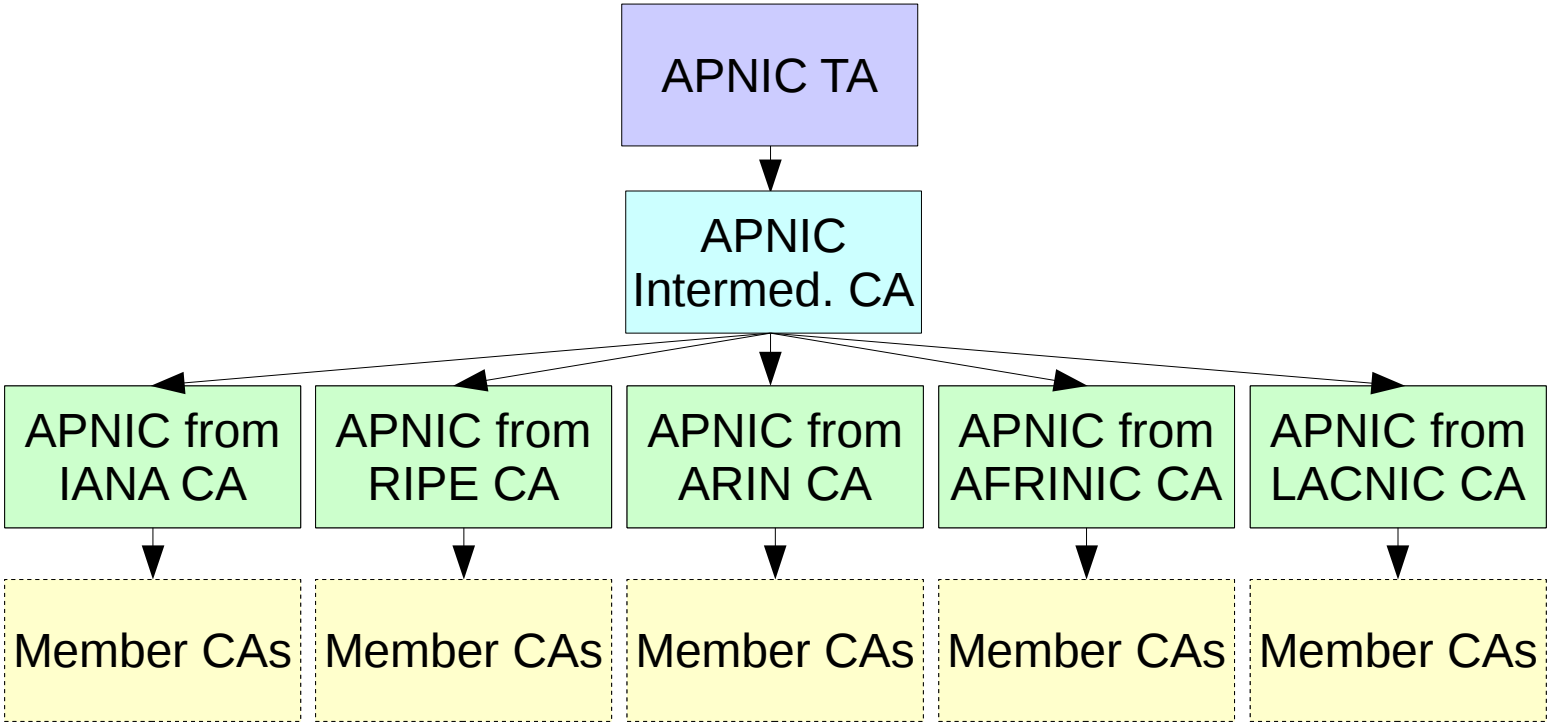
How does the transition happen? (4)



How does the transition happen? (5)



What is the state after the transition?



Why is this happening?

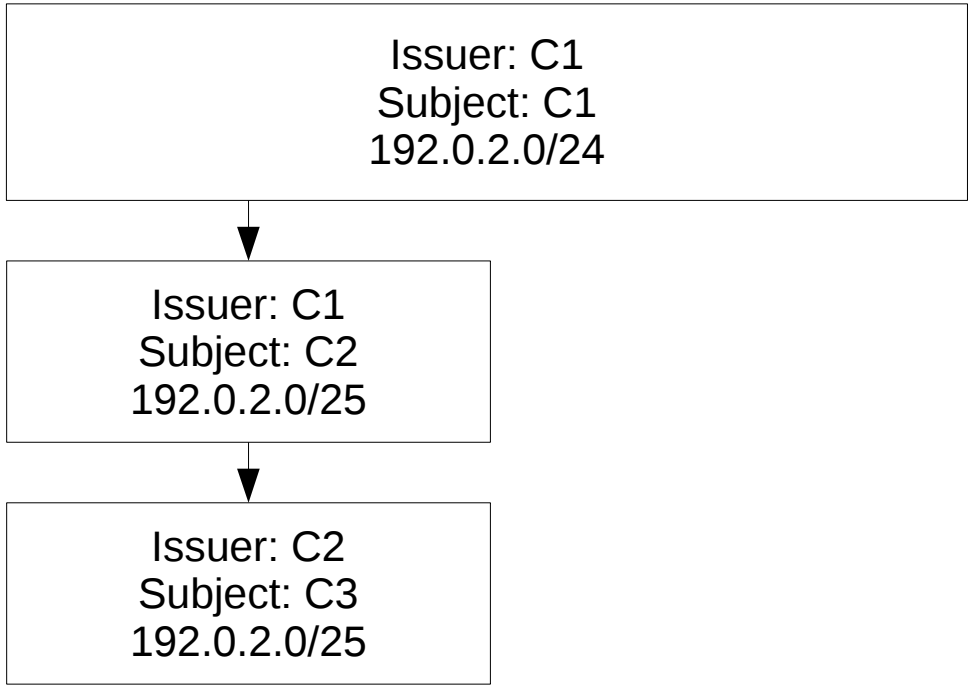
- Increase RIR consistency by aligning on TA approach
- Reduce invalidity risks associated with:
  - Inter-RIR transfers and other changes in resource disposition
  - TA work

How is RIR consistency helped?

- Each of the other RIRs has a single TA
- APNIC has five TAs, because of expectations around system development that were overtaken by events
- This lack of consistency concerns people who might otherwise be interested in using RPKI
- Having each RIR explicitly adopt the same approach deals with this problem

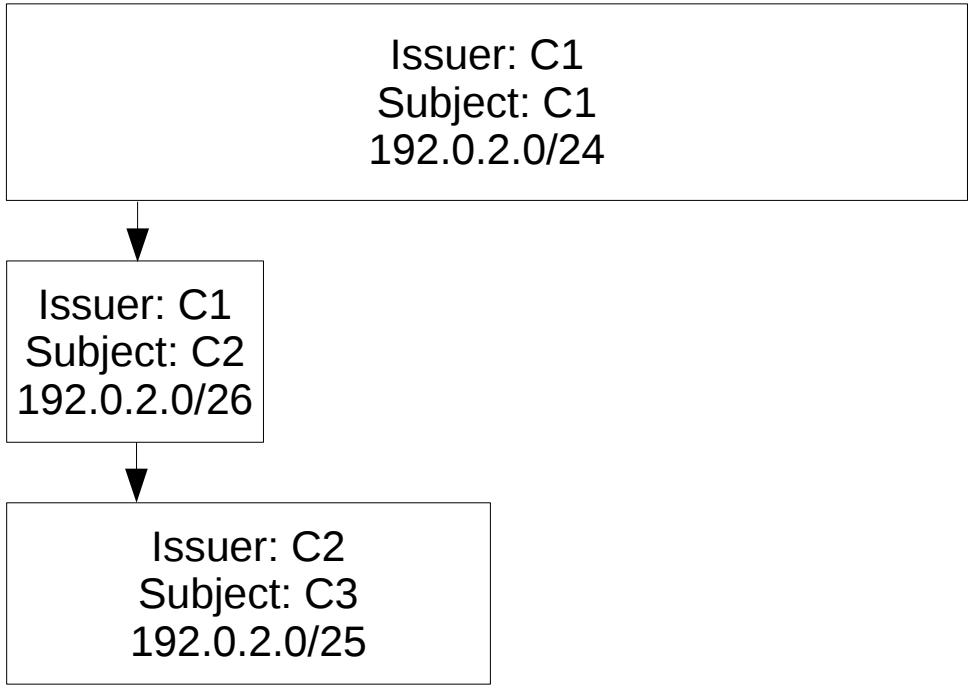
How does RPKI validation work?

- As far as resource holdings are concerned, the issuer must cover all of the resources
- C1 issues /25 to C2, and C2 issues /25 to C3: all certificates valid



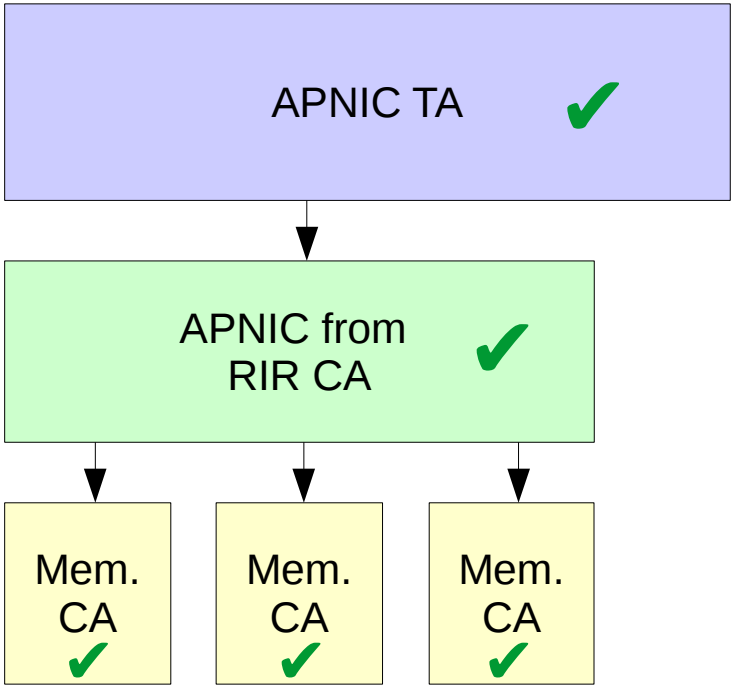
How does RPKI validation work?

- If any of the resources are not covered, the certificate as a whole is invalid
- C1 reissues C2 with /26: C3 now entirely invalid



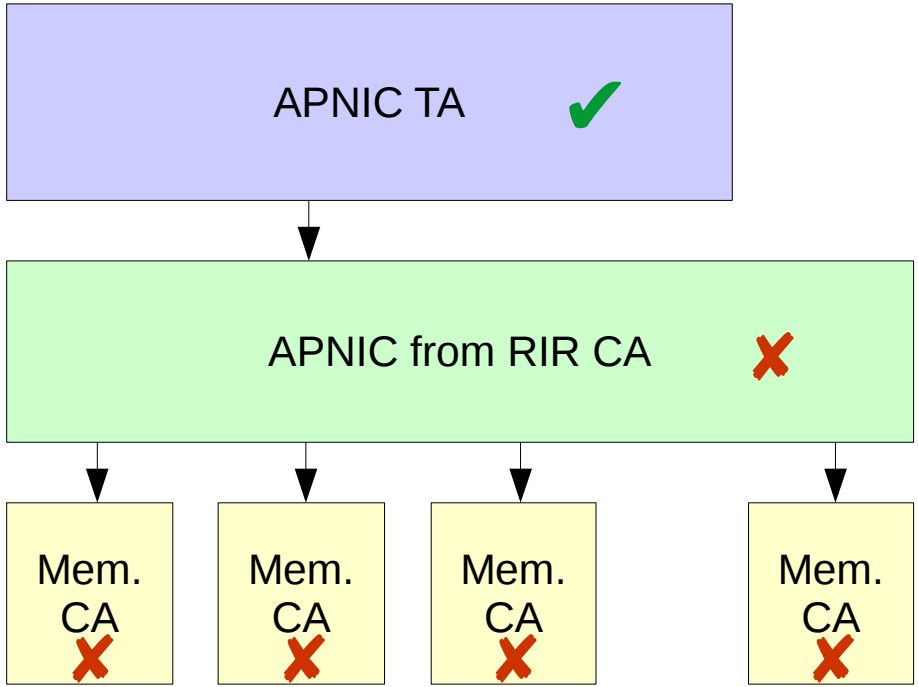
How can transfers affect validity?

- Before inbound transfer: each certificate's resources covered by issuer, so each certificate is valid



How can transfers affect validity?

- Transfer occurs, but operator error/bug leaves TA unpublished
- Online CA overclaims: invalid
- **All** member CAs become invalid, not just those receiving transferred resources

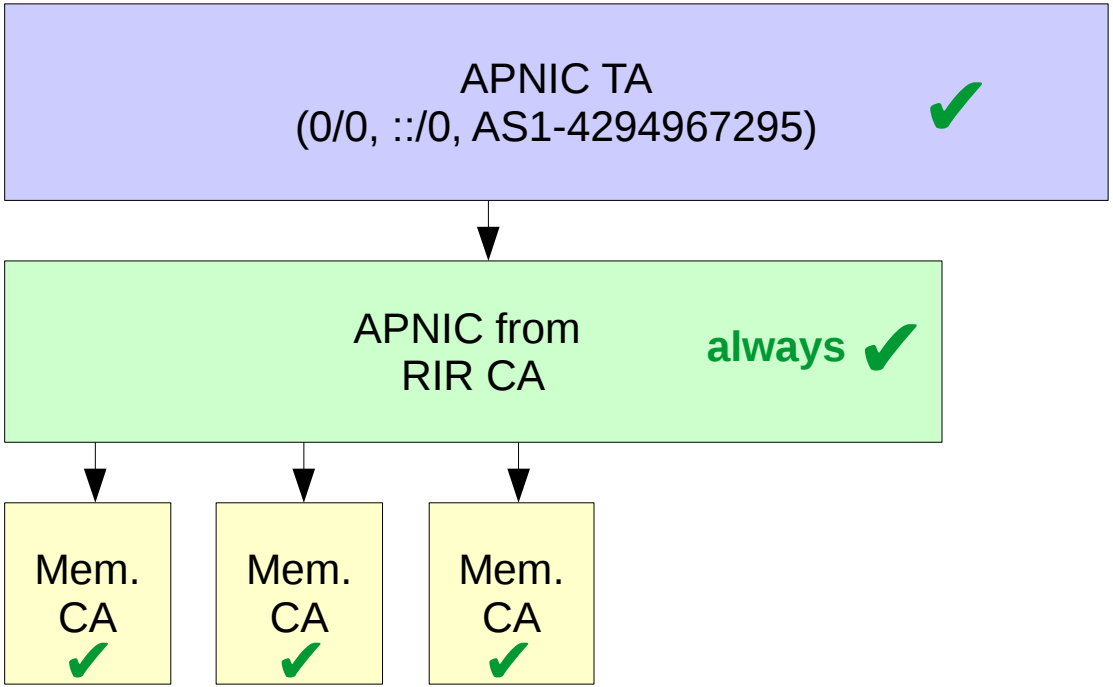


How can this problem be resolved?

- There is a document currently working through the IETF, draft-ietf-sidr-rpki-validation-reconsidered, that allows an overclaiming certificate to be considered valid for those resources that are covered by its issuer
- However, it will be some time before the document is finalised, and longer still until relying party software is upgraded and deployed

How does the transition help this?

- If the TA claims all resources
- Then it's impossible for the online CA to overclaim
- And mass invalidity due to overclaiming can't occur



How can TA work affect validity?

- APNIC's TAs are backed by a Hardware Security Module (HSM), as are those of the other RIRs
- A great deal of care must be exercised when using an HSM
  - For example, devices may have policies such that a certain number of failed authentication attempts leads to irreversible key destruction
- The more TA work that is happening, the greater the risk

How does the transition help this?

- By having the TA be responsible for all resources, the need to do TA work is limited to scheduled and well-understood events:
  - Manifest/CRL reissuance
  - TA reissuance

What do I need to do?

- If you only issue ROAs:
  - No change required
- If you run relying party software:
  - Once APNIC has announced the successful transition, remove the unused TAs from configuration and cache
  - However, leaving them in place will not affect validity outcomes

When will this happen?

- Previously planned for September
- Some problems that were found during the testbed transition mean that deployment has been delayed so that further testing can occur
- An announcement will be made as to a new timeline once that has been confirmed

APNIC 44

#apnic44

TAICHUNG, TAIWAN

7–14 September 2017