MyNOG 2017

APNIC RPKI Service Update

Brenda Buwu, Network Engineer

brenda@apnic.net

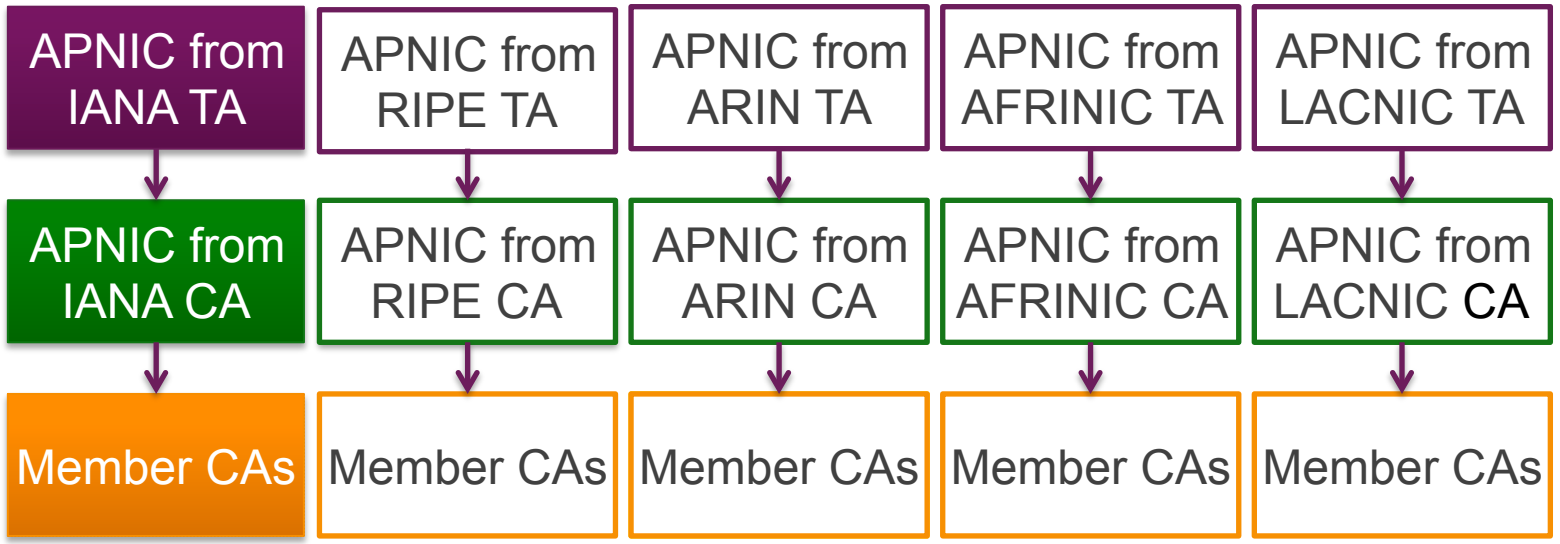
RPKI in Malaysia at a glance

	ASN	IPv4 holders	IPv6 holders
Delegated	199	227	154
Active in RPKI	11	12	5

- Low levels of participation — <10% in all categories
- This is mostly a ‘one click’ activity in MyAPNIC, so easy to engage!
- Percentage coverage of active BGP by address range high: 100% in IPv6, >75% in IPv4
- Please log in to your MyAPNIC account and enable RPKI

It’s your address and routing plan: protect it!

What does the current APNIC RPKI look like?



APNIC is altering its RPKI TA model

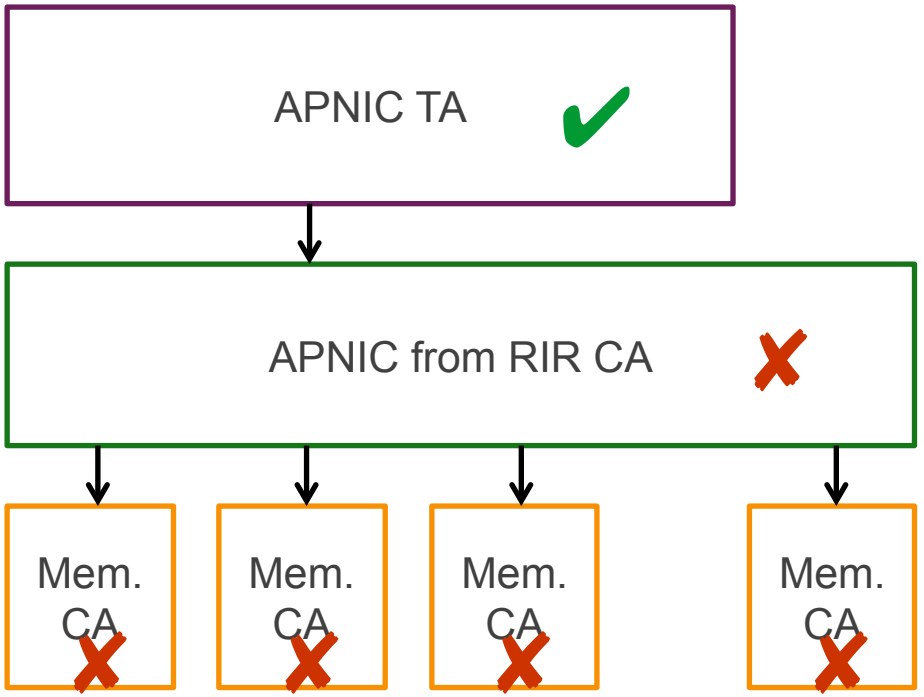
- PKI depends on a **Trust Anchor** (TA) model
  - Validation of all signed objects is under a given TA
  - The TA is external, supplied; foundation of the trust system
- The current APNIC RPKI depends on five TAs
  - Pre-emptively architected to align with real-world and future unified global RPKI model
  - BUT, unification has not emerged; instead complex divergent set of TAs across the five RIRs
  - All RIRs' TAs converging into a single, consistent TA model – each RIR can certify any resource

Why is this happening?

- Increase RIR consistency by aligning on TA approach
  - We will now operate a mutually consistent model
- Reduce invalidity risks:
  - Internet transfers (inter and intra) are frequent — resources are coming into or leaving any given RIR each month
  - Necessitates changes in the TA to reflect these shrinkages and growth events
  - Each transaction is a risk window for a process failure
  - TA work is now far less frequent; no changes as resources move between RIRs, or are assigned by IANA

How can transfers affect validity?

- Transfer occurs, but operator errors/bugs leaves TA unpublished
- Online CA over-claims: invalid
- **All** Member CAs become invalid, not just those receiving transferred resources



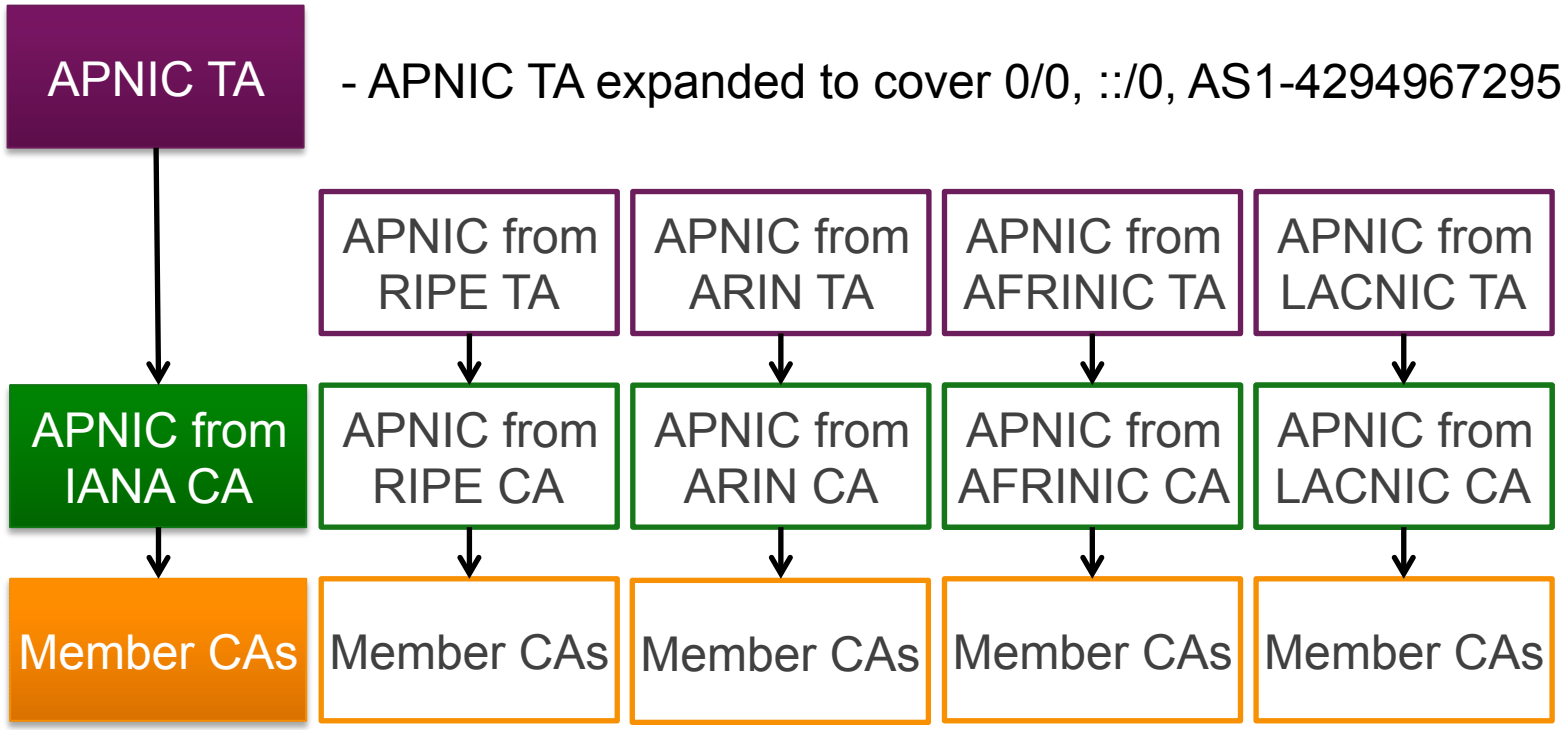
How can this problem be resolved?

- Draft IETF document (draft-ietf-sidr-rpki-validation-reconsidered) allowing an over-claiming certificate to be considered valid for those resources that are covered by its issuer
- But still some time before the document is finalized, and longer still until relying party software is upgraded and deployed

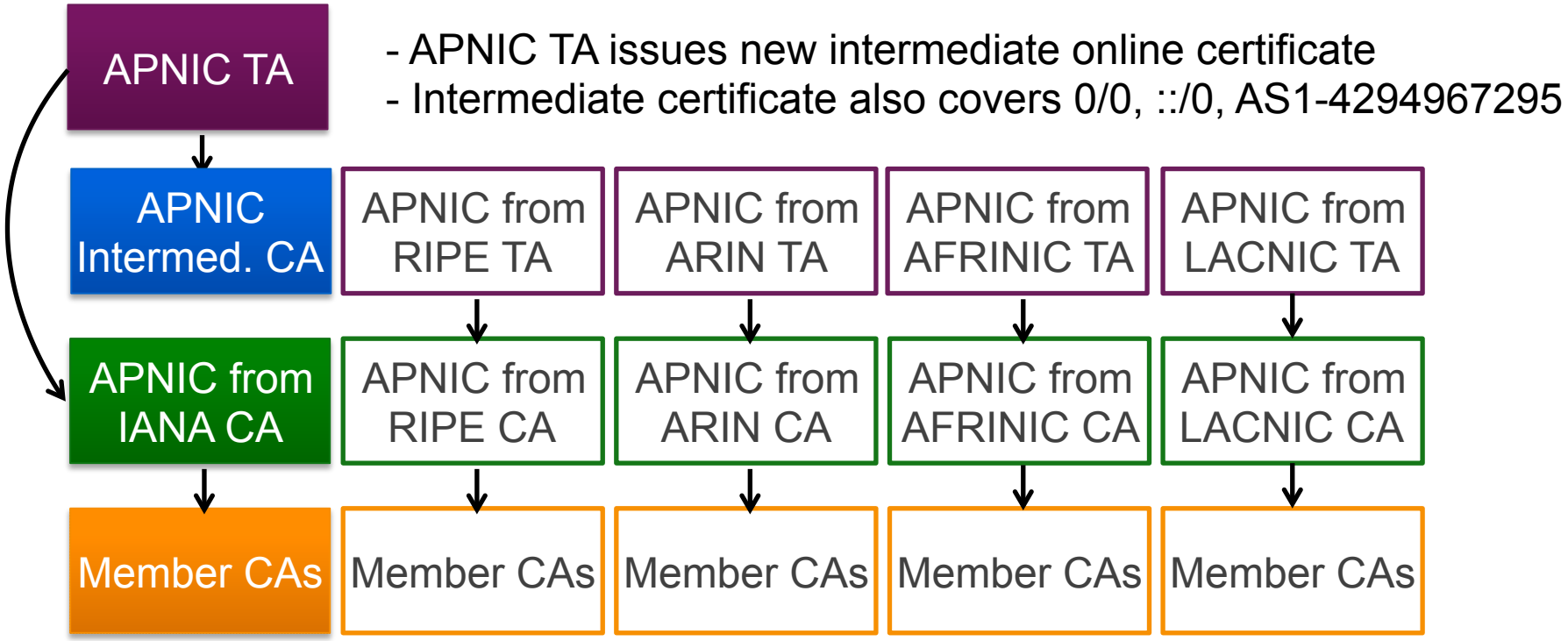
Failure in RPKI has wide consequences

- Operational failure high in the tree is catastrophic
  - All resources under that arc of a tree (for a TA, all resources!) are invalid
- Each transaction is a risk window for a process failure
  - All failures in the APNIC TA risks invalidating all products across the Asia Pacific
  - APNIC felt this risk was unacceptable
- APNIC has decided to re-architect to a model that removes this risk, and also removes operational complexity under transfers
- Reunify under one TA — make that TA ‘all resources’

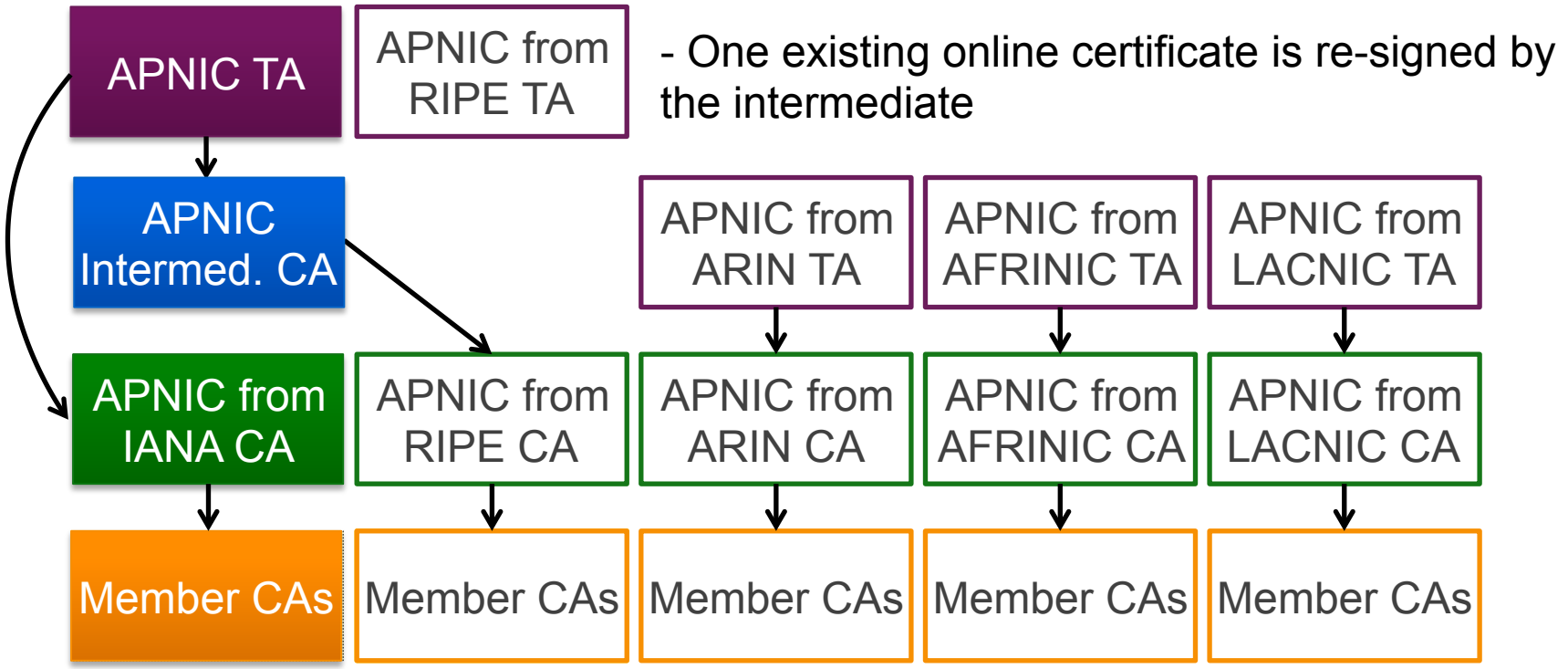
How does the transition happen? (1)



How does the transition happen? (2)

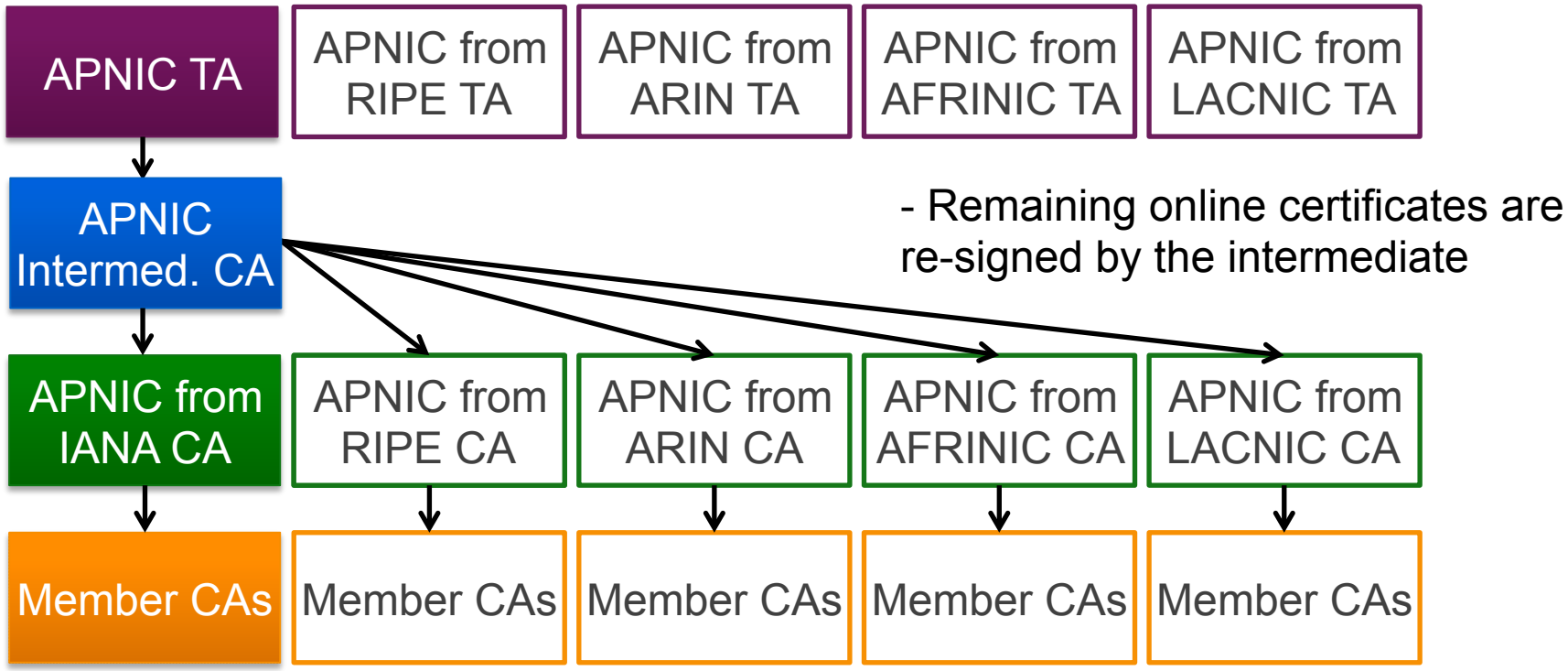


How does the transition happen? (3)

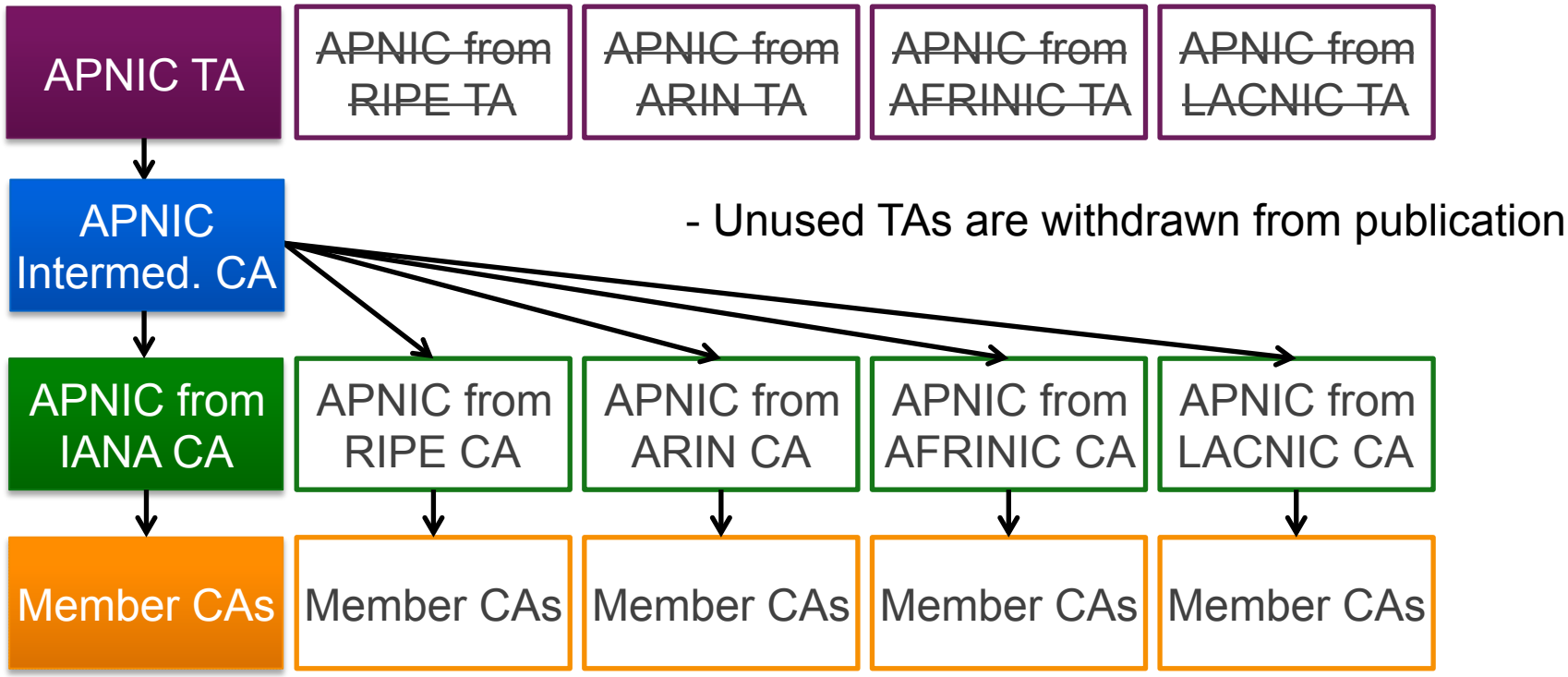


- One existing online certificate is re-signed by the intermediate

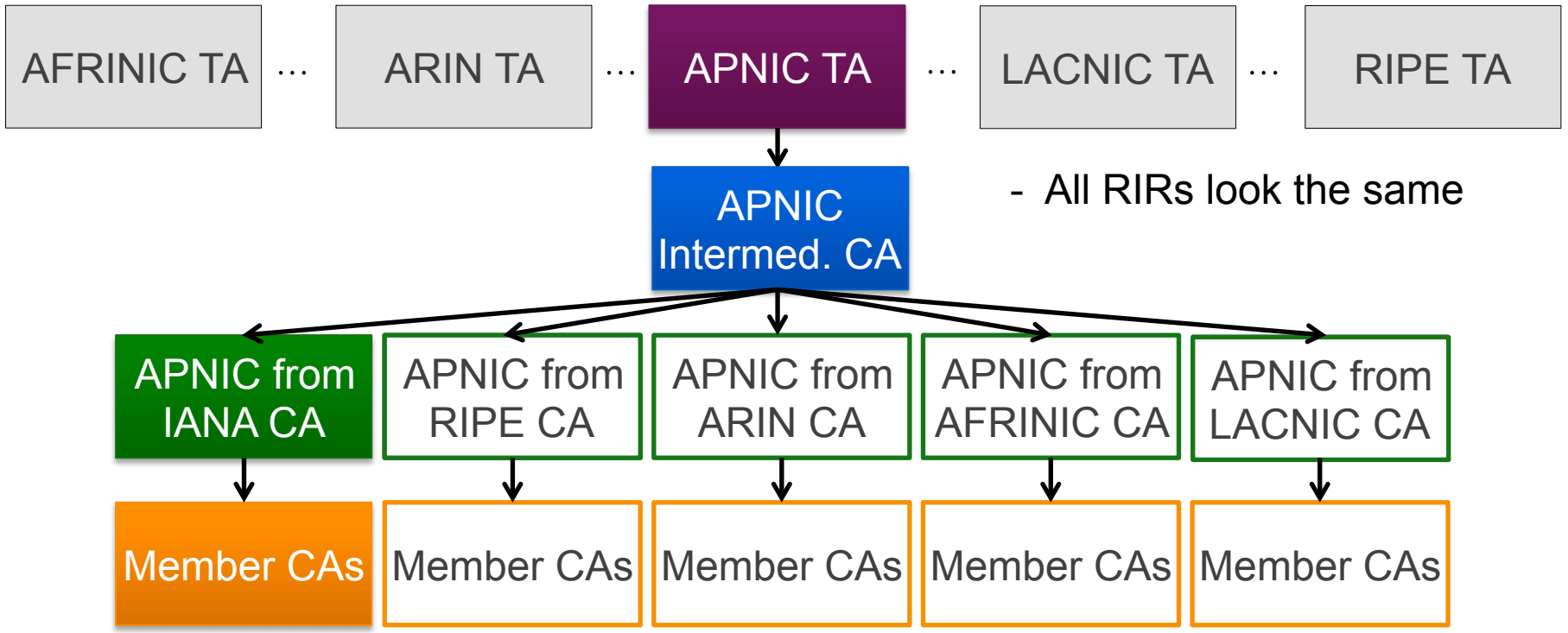
How does the transition happen? (4)



How does the transition happen? (5)

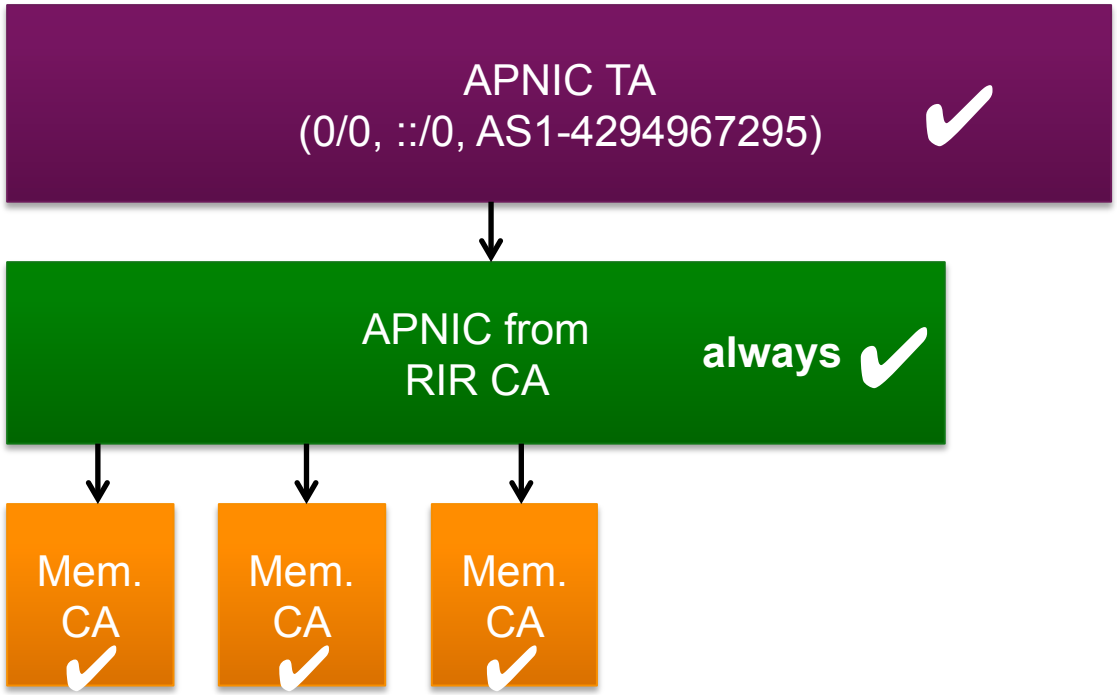


What is the state after the transition?



How does the transition help this?

- If the TA claims all resources, it's impossible for the online CA to over-claim
- Mass invalidity due to over-claiming 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 meant that deployment has been delayed so that further testing can occur
- Update to the new single-TA model is expected to be completed by the end of October
- The four unused TAs will be withdrawn in 2018

https://www.apnic.net/single-ta-transition

Thanks!