RPKI ROAs for Unallocated and Unassigned AFRINIC Address Space

Implementation options

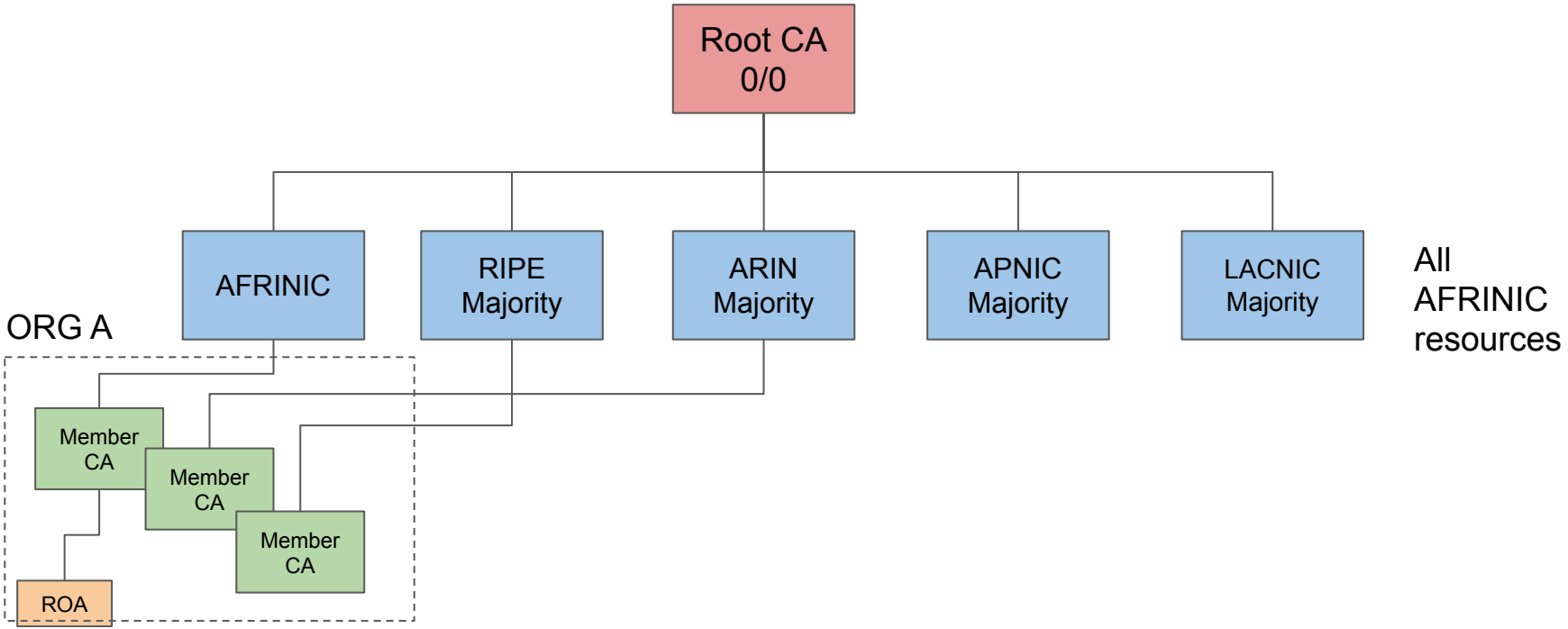
DBWG

30 September 2020

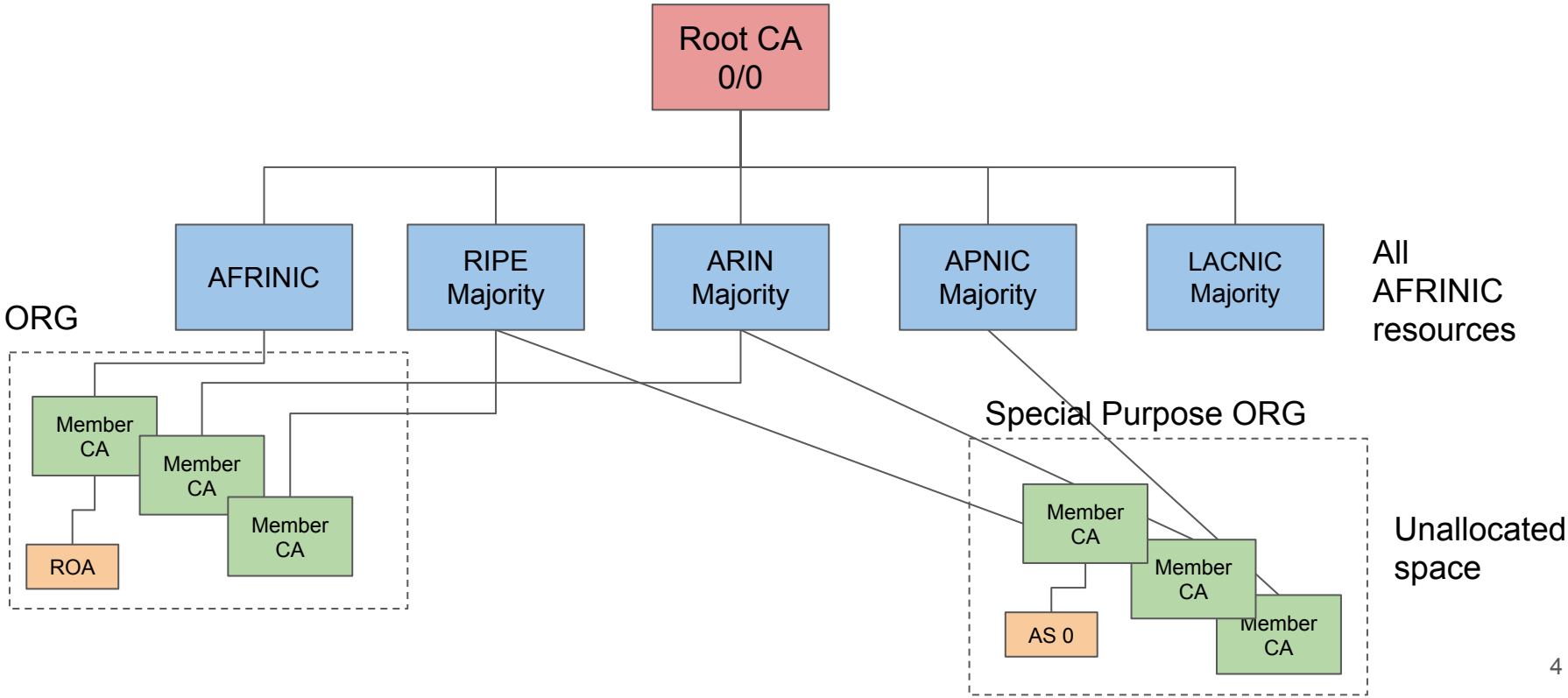
Policy proposal (status: under discussion)

- AFRINIC must create ROAs with origin AS0 for all the unallocated and unassigned address space (IPv4 and IPv6)
- AFRINIC must revoked AS0 ROA before allocation/assignment to resource member
- Address space can only be allocated once the ROA or ROAs with origin AS0 have been fully removed and are not visible in the repositories.
- AS0 ROAs could be under a distinct Trust Anchor Locator (TAL), so it becomes an opt-in service and provides separate measurements, at least in the initial deployment phases. This and other operational details are left to the discretion of AFRINIC.

Current RPKI architecture



Option A - Special Purpose ORG



Analysis - A

- Need to create a SPO on MyAFRINIC/WHOIS and allocate the “available” space to that ORG
- MyAFRINIC business rules to be updated to allow this org to create AS0 only and not any other ROA
- Impact on RPKI **LOW**
- Impact on MyAFRINIC **Medium**

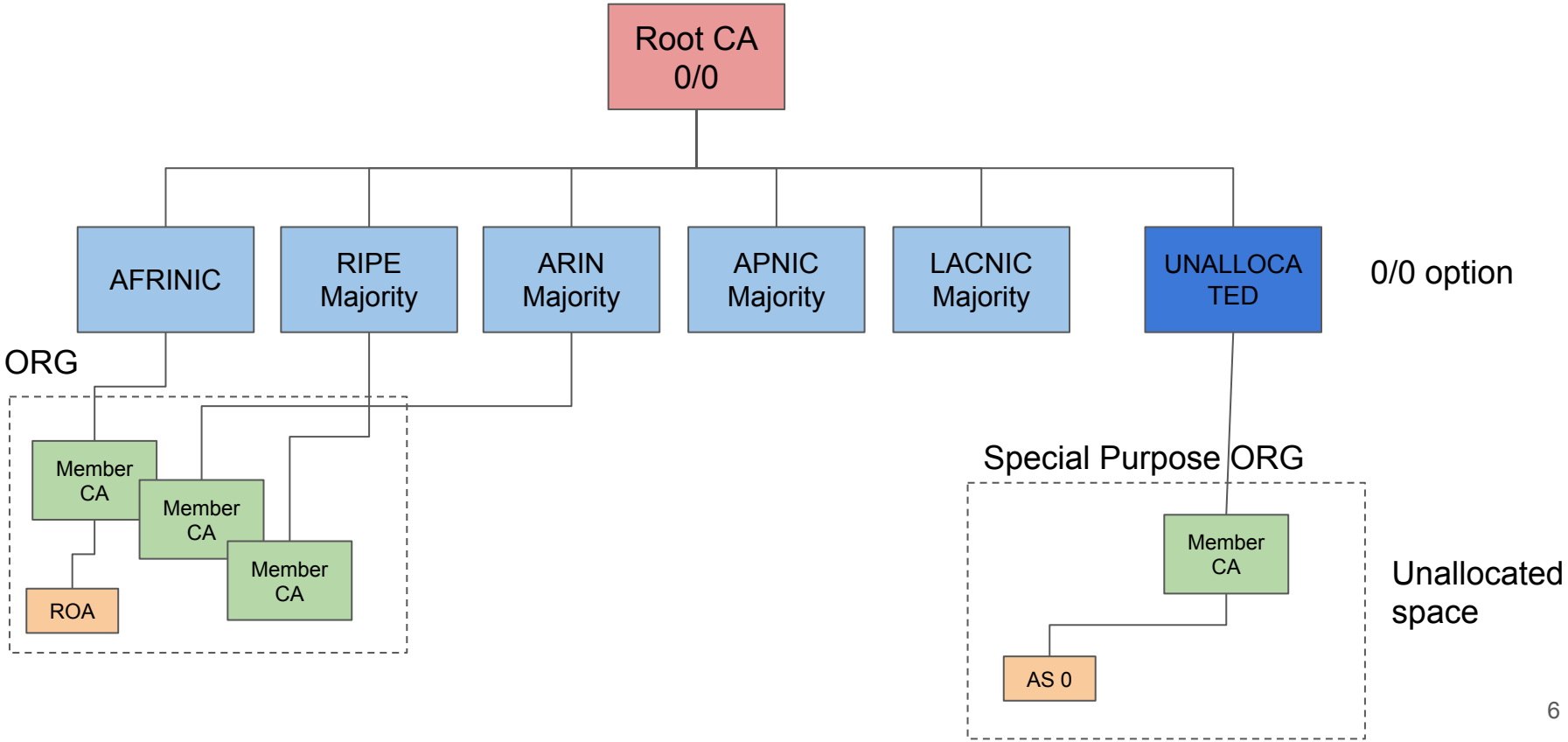
Pros:

- No change on RPKI infrastructure
- AS0 will be published in the same RPKI repository and will therefore benefit from the same reach as the existing repository

Cons:

- Relying parties cannot opt-out. They will have to accept the "AS0 for unallocated" ROAs as any normal AS0 ROA.

Option B - Unallocated CA + Special Purpose ORG



Analysis - B

- Need to create a SPO on MyAFRINIC/WHOIS and allocate the “available” space to that ORG
- MyAFRINIC business rules to be updated to allow this org to create AS0 only and not any other ROA
- UNALLOCATED CA needs to be refreshed everytime there is a change in the unallocated pool **HIGH**
- Impact on MyAFRINIC **Medium**

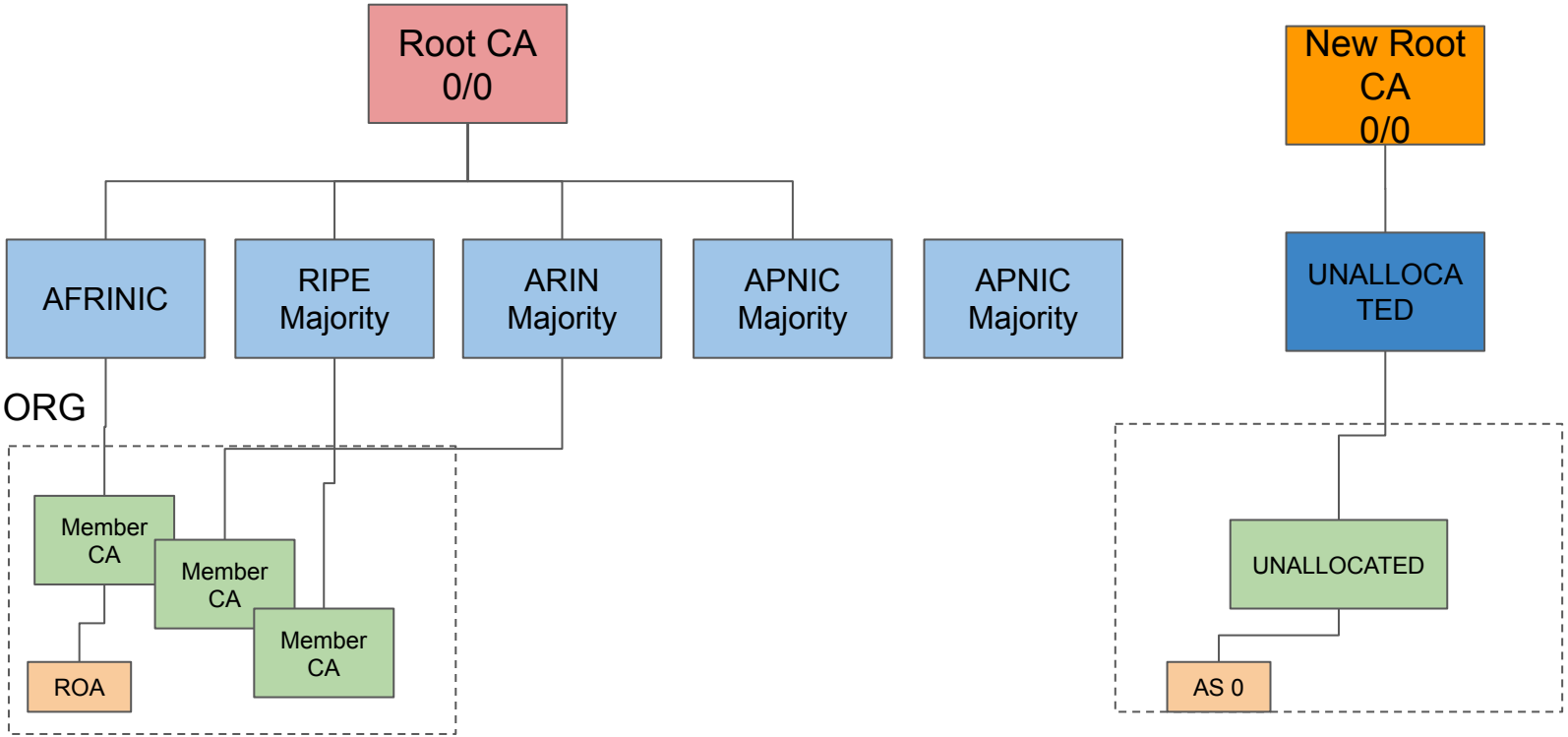
Pros:

- AS0 will be published in the same RPKI repository and will therefore benefit from the same reach as the existing repository

Cons:

- Relying parties cannot opt-out. They will have to accept the "AS0 for unallocated" ROAs as any normal AS0 ROA.

Option C - New TAL



Analysis - C (Recommended)

- Completely independent TAL
- CA software for “Unallocated CA” also decoupled from main RPKI and MyAFRINIC
- UNALLOCATED-CA will talk to the AFRINIC inventory system to retrieve latest changes
- ROA published in a separate repository
- Impact on MyAFRINIC **LOW**
- Impact on existing RPKI **LOW**
- New RPKI tree to maintain **HIGH**

Pros:

- Low impact on existing systems
- Separate CA and repository

Cons:

- Two RPKI tree with the same resources, potential room for conflicting ROAs
- OPT-IN: installing this TAL is therefore optional

Questions

amreesh@afrinic.net