Multicast Router Key Management Protocol (draft-hartman-karp-mrkmp and draft-tran-karp-mrmp)

March 28, 2012

Key management for routing protocols using multicast

- MarK defines a state machine and election process for choosing a key server
- G-IKEv2-MRKM defines authentication and key management for a group of routers

The authors agreed to combine the 2 drafts into a single method and will produce a new integrated document.

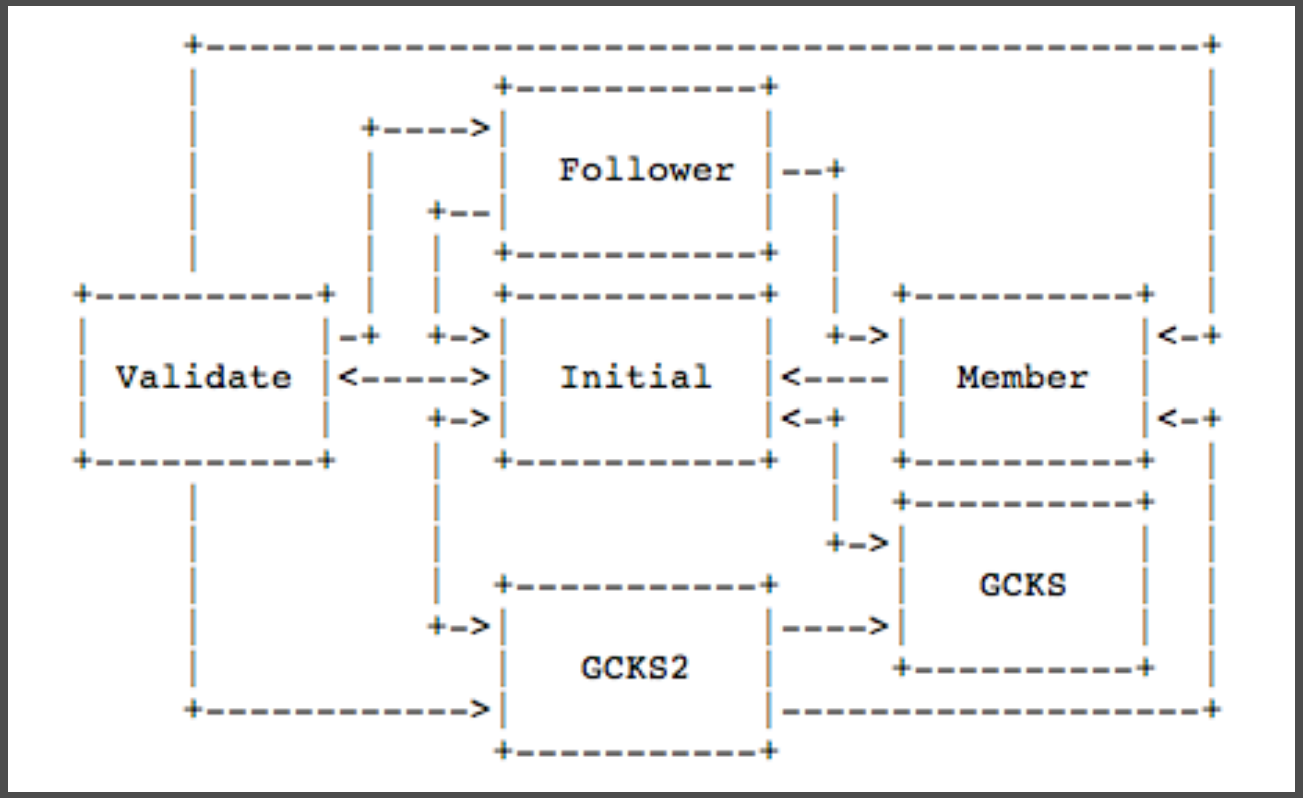
Progress

- Authors identify the sections of MaRK that should use the G-IKEv2 MRKM exchange
- We also discovered an opportunity to come up with a simpler state machine

State machine options

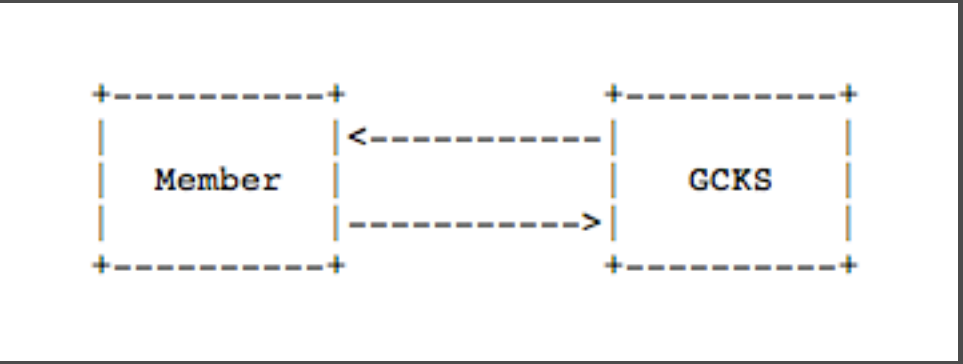
- Option 1: Highest priority router will become the key server if there's a cold start
- Option 2: Should result in a faster convergence time and is simpler

Option 1 state machine



Router starts in Initial state and a router moves through the state machine to either member or GCKS depending on its priority.

Option 2 state machine



Router starts up in GCKS state.

When there's more than one GCKS, they elect one GCKS and the loser becomes a member.

When the GCKS disappears the member with the highest priority will become GCKS.

Request Input

We are looking for input from the working group of how important it is for the highest priority router to become the key server

- Should this semantic be prioritized higher than convergence time?

Next Steps

- Integrate G-IKEv2-MRKM into the MaRK architecture
- Authors plan to have a combined document available before the Vancouver IETF 84 meeting