sidrops@IETF'102
Montreal, July 2018

draft-ieft-sidrops-rpkimaxlen-00

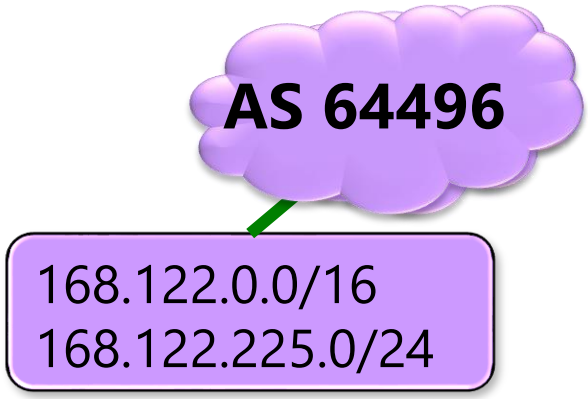
Use of MaxLength in the RPKI

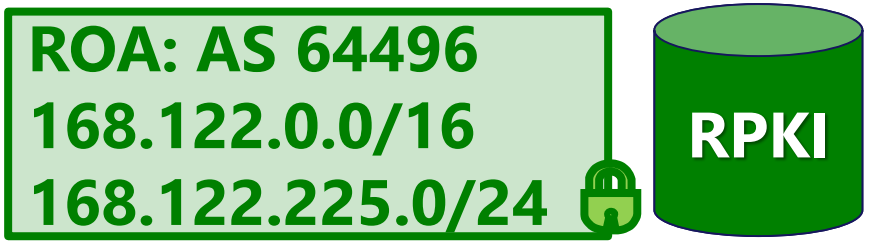
BCP draft update

Yossi Gilad (Boston University)
Sharon Goldberg (Boston University)
K. Sriram (NIST)
Job Snjiders (NTT)
Ben Maddison (Workonline Communications)

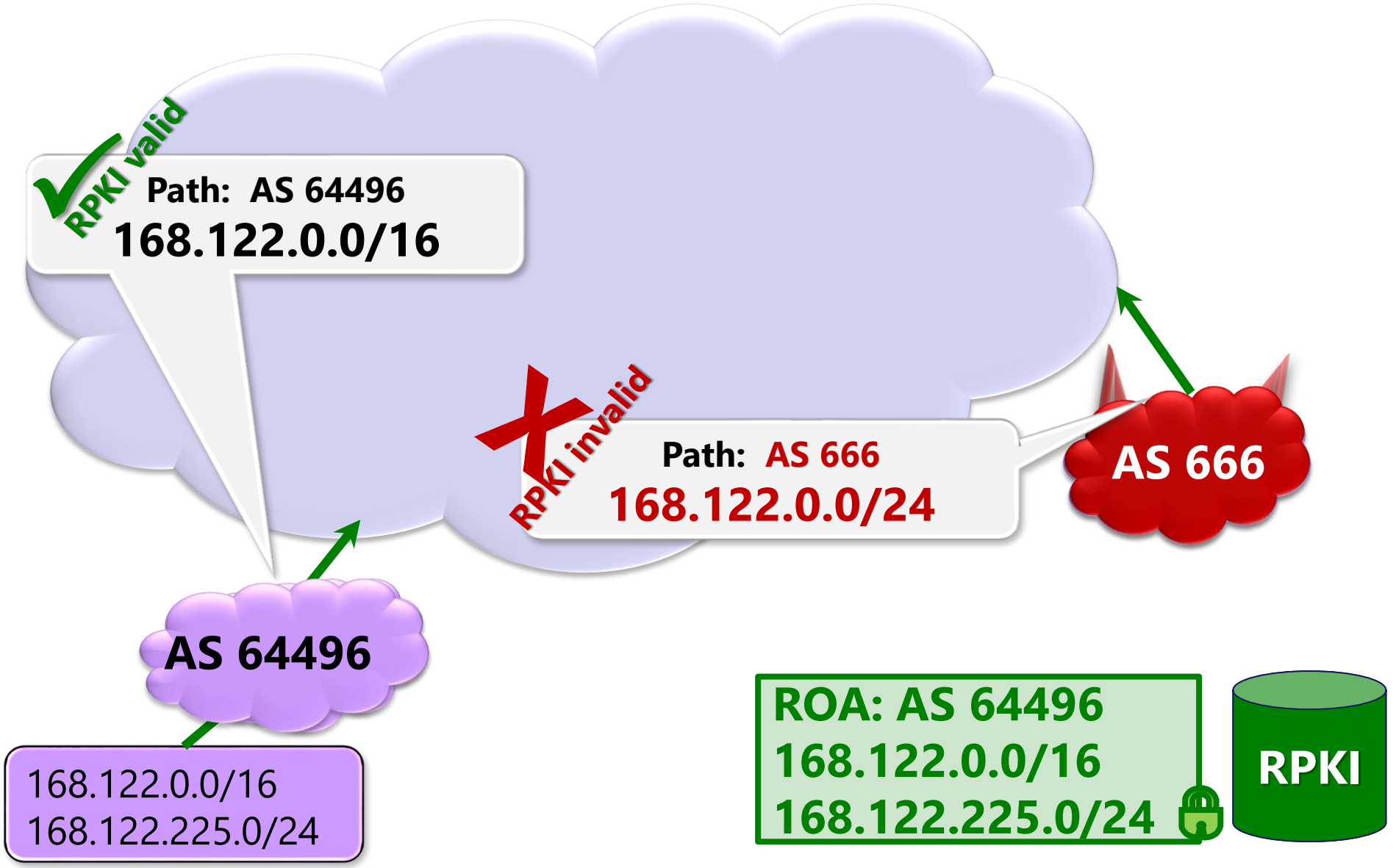
“minimal ROAs”

This ROA is "minimal" because it includes only those IP prefixes that AS 64496 originates in BGP, but no other IP prefixes [RFC6907].





minimal ROAs stop subprefix hijacks

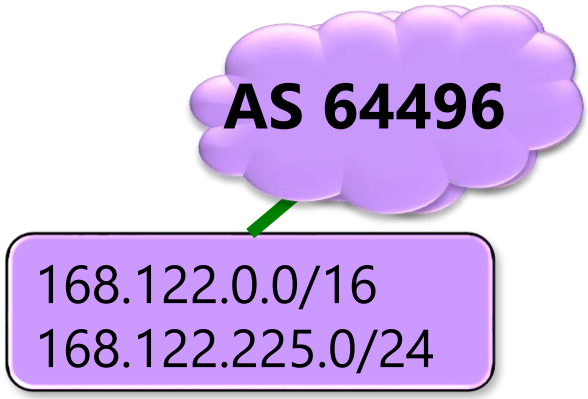


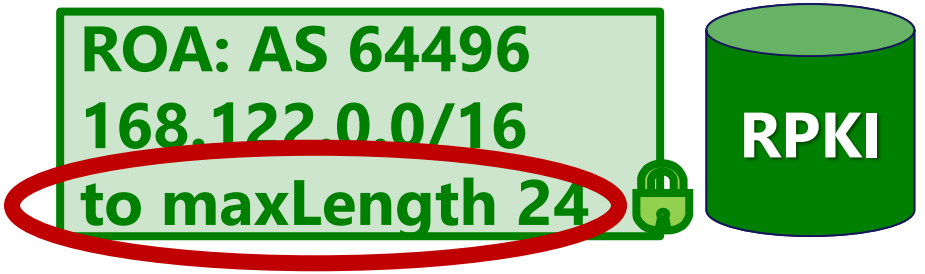
a “loose ROA” using maxLength

This ROA uses maxLength.

This ROA is covers all prefixes announced by AS 64496.

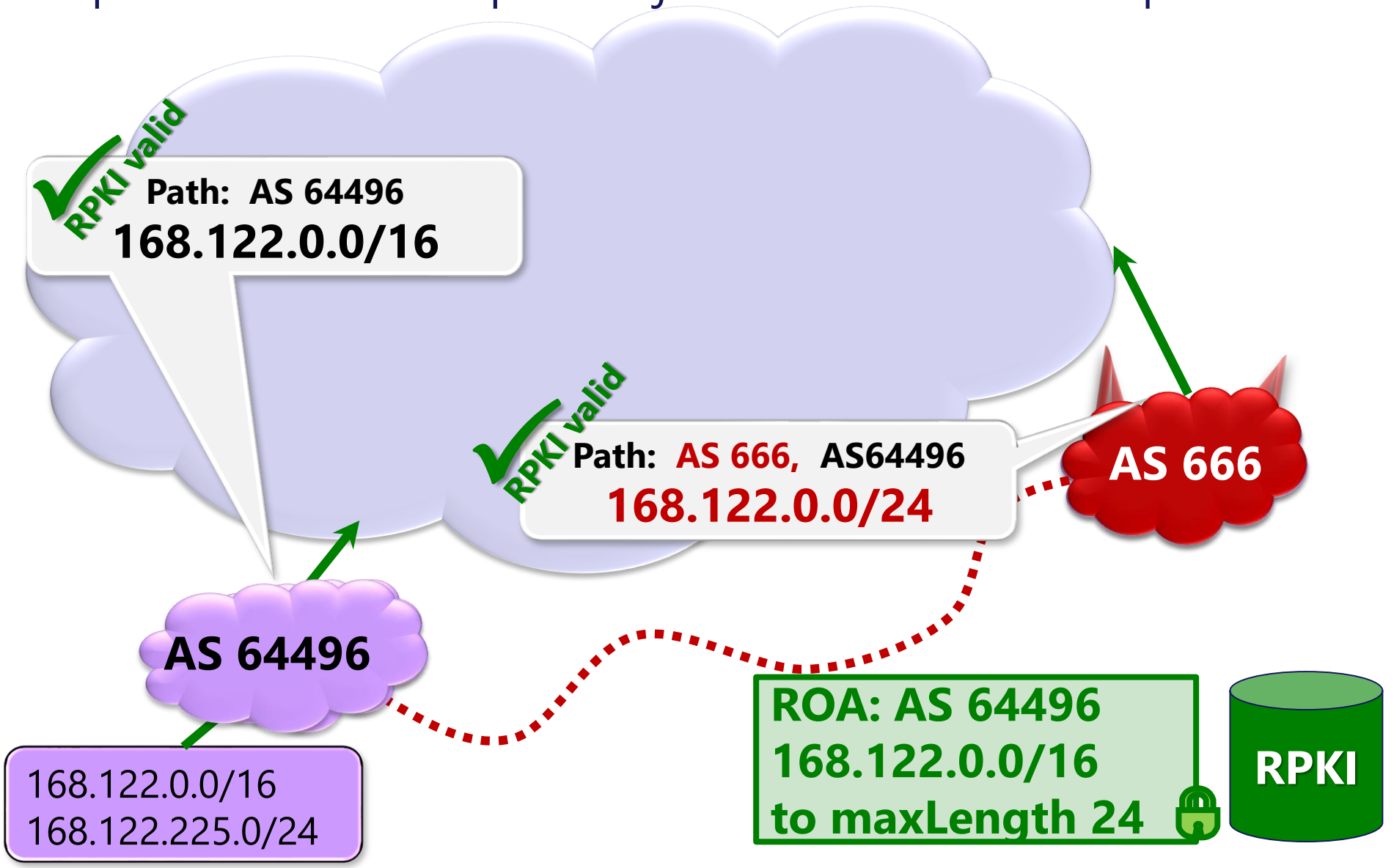
This ROA is not "minimal“ because it covers prefixes that are not originated by AS 64496.





loose ROAs don't stop forged-origin subprefix hijacks

Impact is same as subprefix hijack in absence of ROA protection



key recommendations in the draft

- Operators SHOULD use "minimal ROAs" whenever possible.
- Operators SHOULD avoid using maxLength in ROAs.
  - One ideal place to implement this recommendation is in the user interfaces for configuring ROAs.
  - Designers and/or providers of ROA config interfaces SHOULD provide warnings to draw the user's attention to the risks of using the maxLength attribute.
- This practice requires no changes to the RPKI specification and will not increase the number of signed ROAs in the RPKI, because ROAs already support lists of IP prefixes [RFC6482].

recommendation: when you can’t use a minimal ROA

- Sometimes, it is not possible to use a "minimal ROA", because an operator wants to issue a ROA that includes an IP prefix that is sometimes (but not always) originated in BGP.
- In this case, the ROA SHOULD include
  - the set of IP prefixes that are always originated in BGP, and
  - the set IP prefixes that are sometimes, but not always, originated in BGP.
- The ROA SHOULD NOT include any IP prefixes that the operator knows will not be originated in BGP.
- Whenever possible, the ROA SHOULD avoid use of maxLength

questions?