# Local Management of Trust Anchors for the RPKI (status update)

Stephen Kent

BBN Technologies

# Local TA Management

- A TA is a public key and associated data used as the starting point for certificate path validation
- It need not be a self-signed certificate (although I am told that OpenSSL requires this format!)
- An underlying assumption in PKI standards is that each relying party selects the trust anchors it will use
- Thus the set of TAs employed by a PKI-enabled application is a local matter
- In practice, few PKI-enabled applications provide users with good tools for managing TAs!

# TAs in the RPKI

- The RPKI architecture follows the general PKI model with respect to TAs, i.e., it assumes each relying party (RP) selects its own set of TAs
- In the RPKI, a TA must include a public key, a subject name, and RFC 3779 extensions, at a minimum
- Thus an RP must be able to create compatible TAs
  - To allow use of local address space for (local) routing
  - To reflect local security decisions about TAs, while still maintaining compatibility with RFC 3779 certificate processing
- This motivates creating a tool to help RPs manage TAs

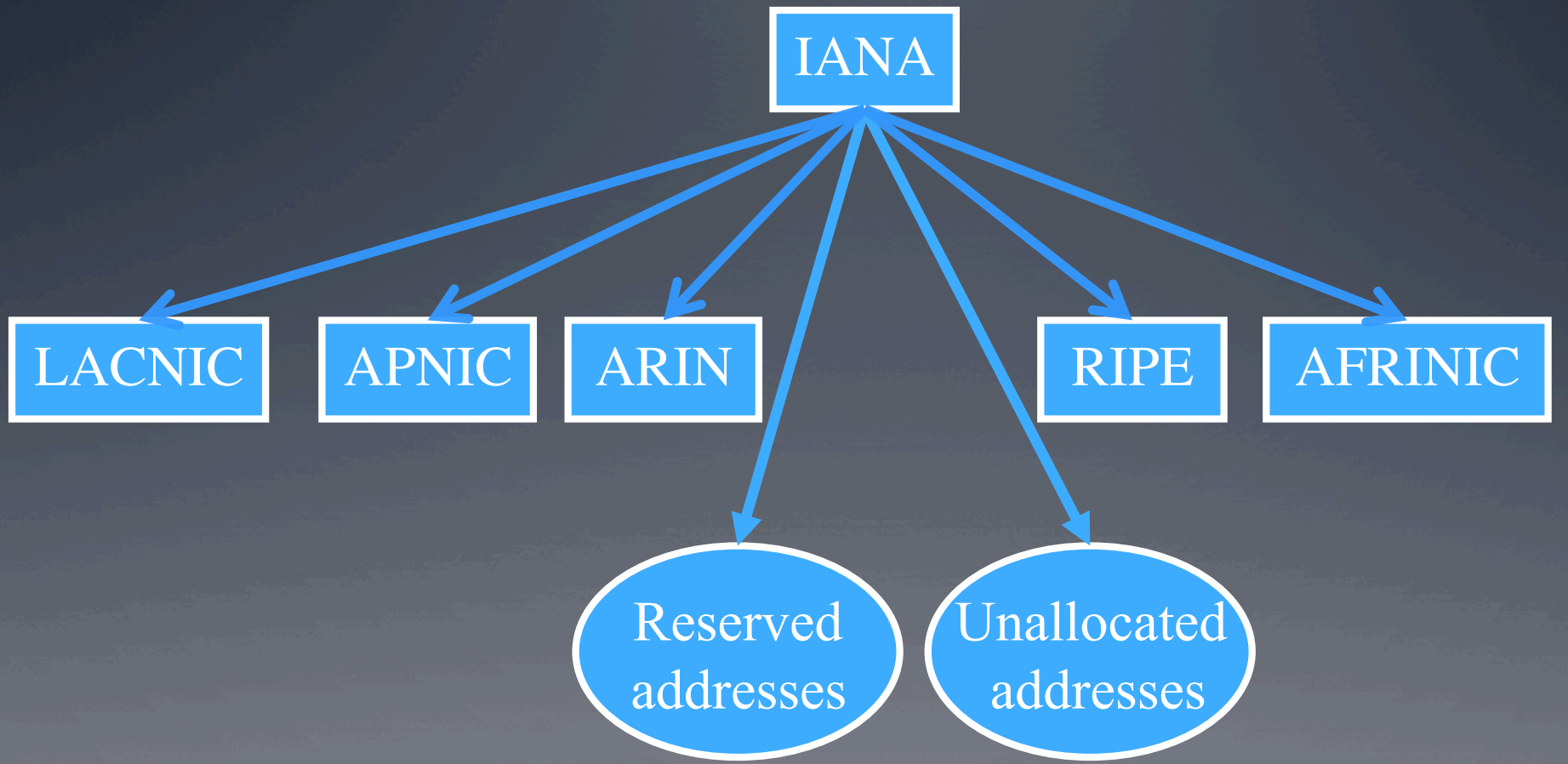
# The RP as the TA!

- The model we propose calls for each RP to recognize exactly one TA, itself!
- The RP imports putative TAs (typically in the form of self-signed certificates) and re-homes them under itself
- The RP can thus override the RPKI nominal hierarchy, as represented in the repository system (paralleling the allocation hierarchy)

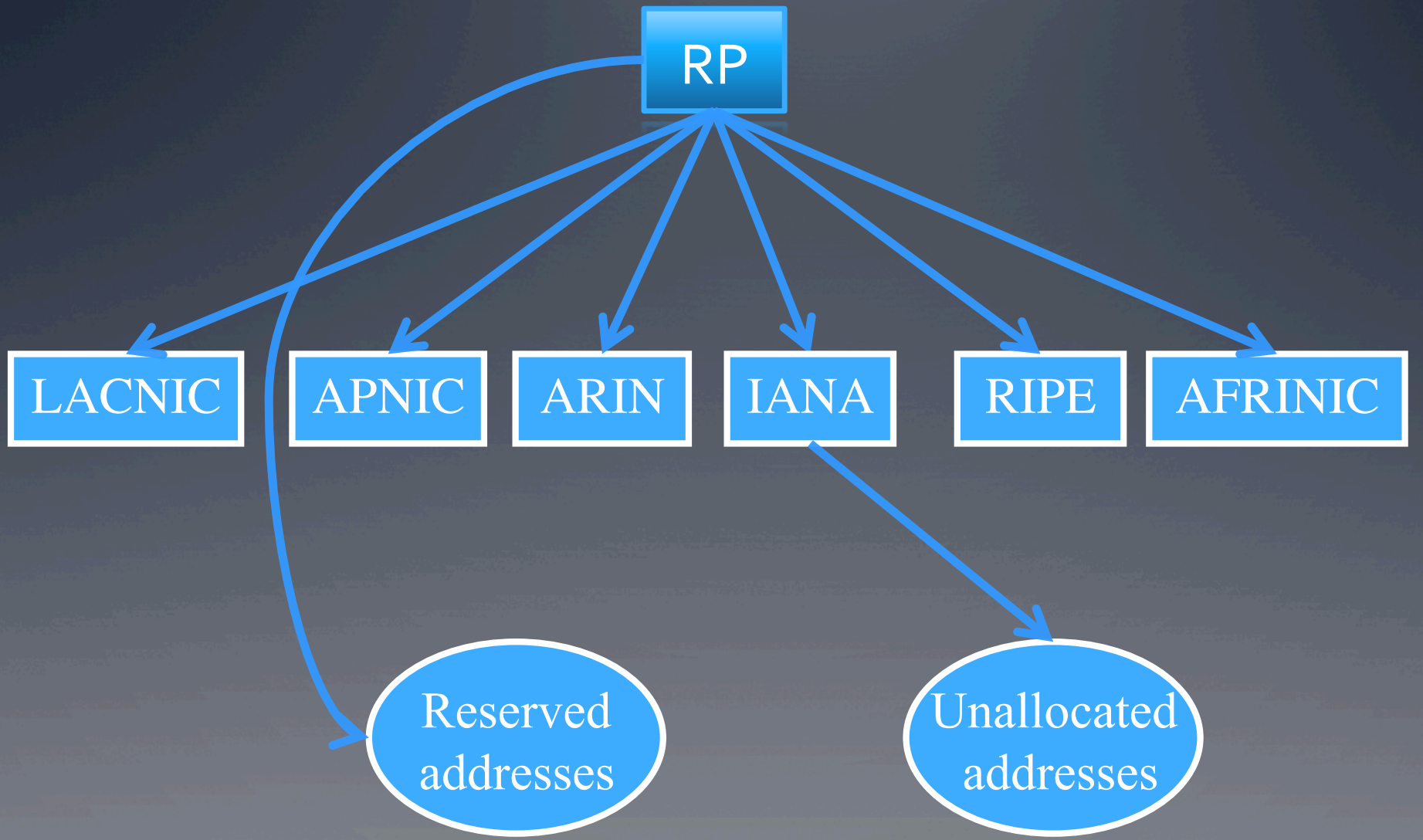
# Making this work in the RPKI

- We will need to be able to create new certificates, often with modified RFC 3779 extensions
- To make this work
  - The self-signed RP certificate must contain RFC 3779 extensions encompassing all addresses and all ASNs
  - Issue new certificates, under the RP's TA, excluding any 3779 extension data that the RP wants to control directly
  - The RP Re-issues certificates with new 3779 extensions to override the RPKI tree
    - Delete overlapping 3779 data as needed
    - Re-homing targeted certificates under the RP TA
    - Re-homing ancestors of re-parented certificates under the RP TA

# An RPKI TA Example



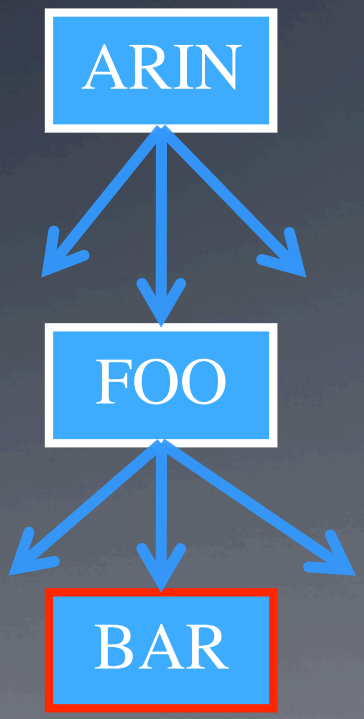
# RPKI with Local Control



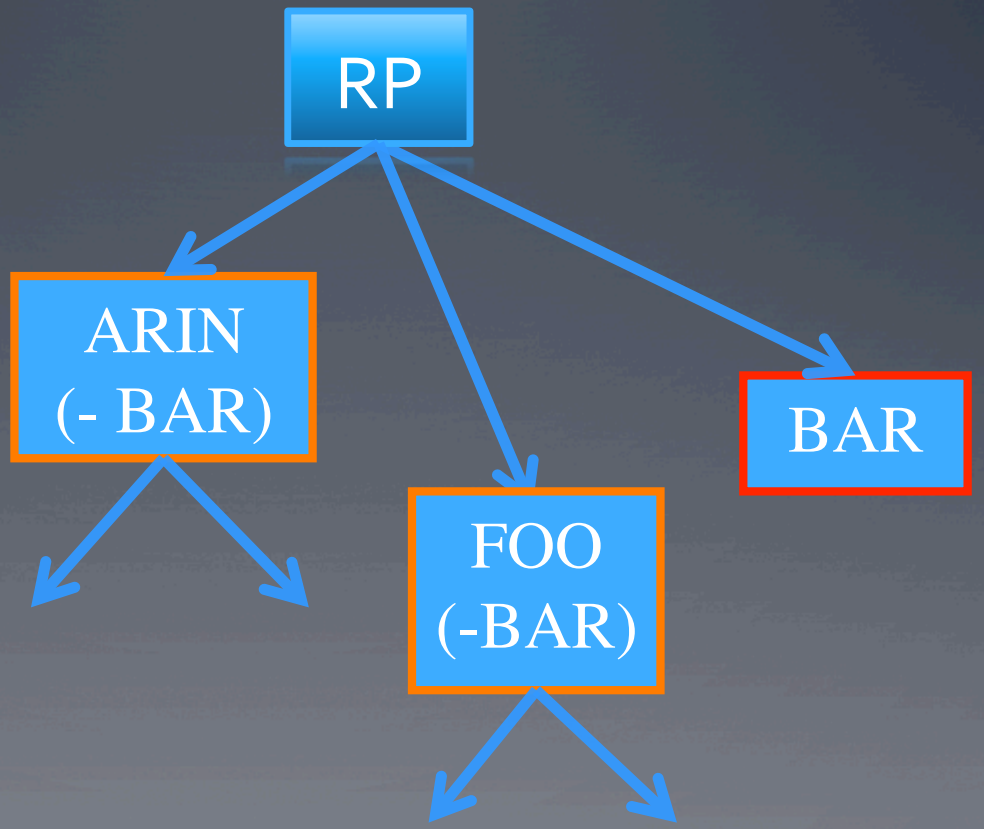

**(RP wants to make use of 10/8 for local routing)**

# A More Detailed Example

As offered by ARIN




As managed by an RP




**(RP trusts its own knowledge of BAR's address allocation and does not want any action by ARIN or FOO to override that knowledge)**

# What does this do?

- It allows each RP to override the nominal RPKI hierarchy, on a local basis
- It is easy to manage if you want to override resource allocations only for local resources (i.e., your allocations) or IANA “reserved” allocations
- It is somewhat harder to manage IF you want to create direct links to many CAs, especially at lower tiers in the hierarchy
- BBN plans to submit an I-D describing how to do this in more detail, before the end of the year