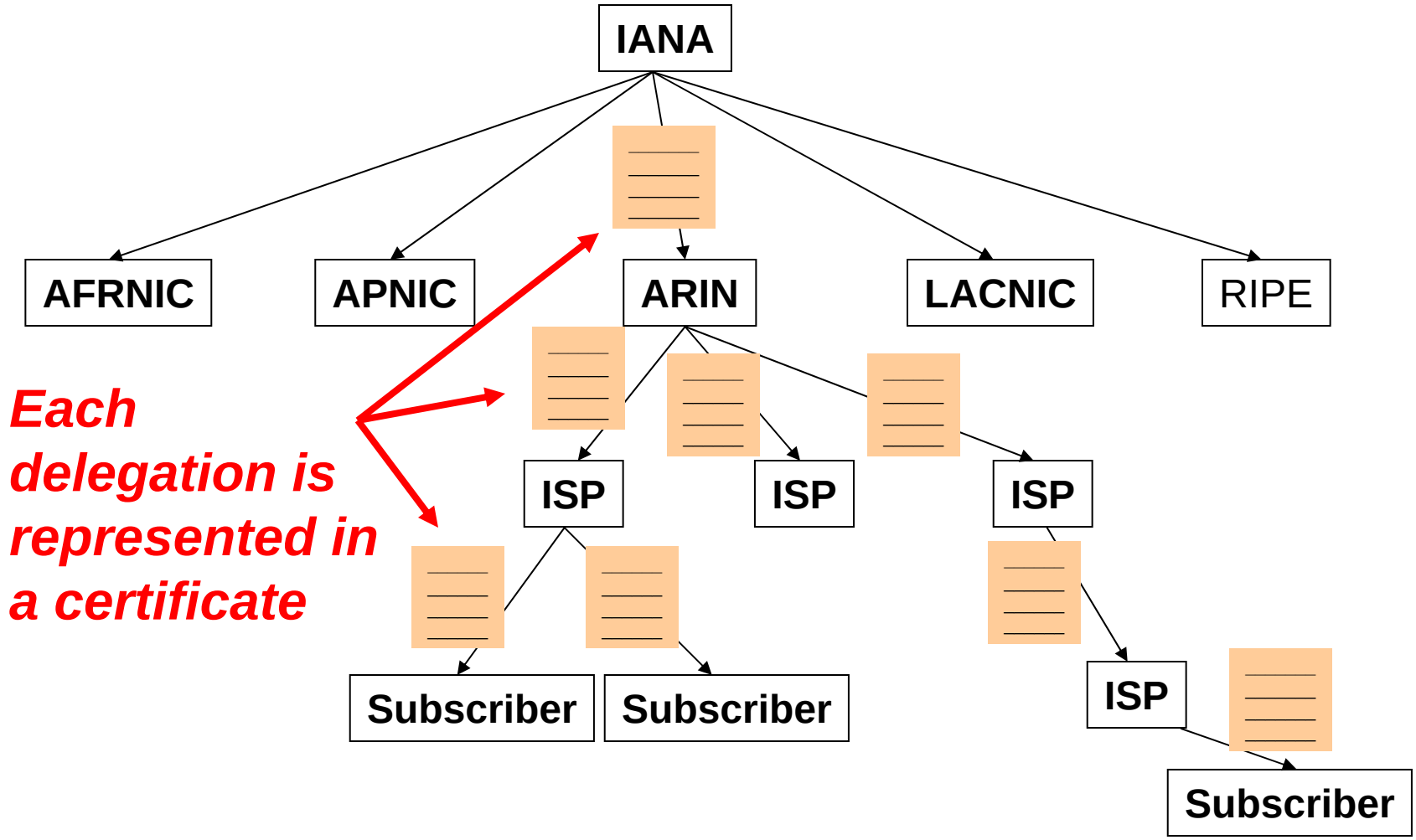
Progress in IETF SIDR wg

Sandra Murphy

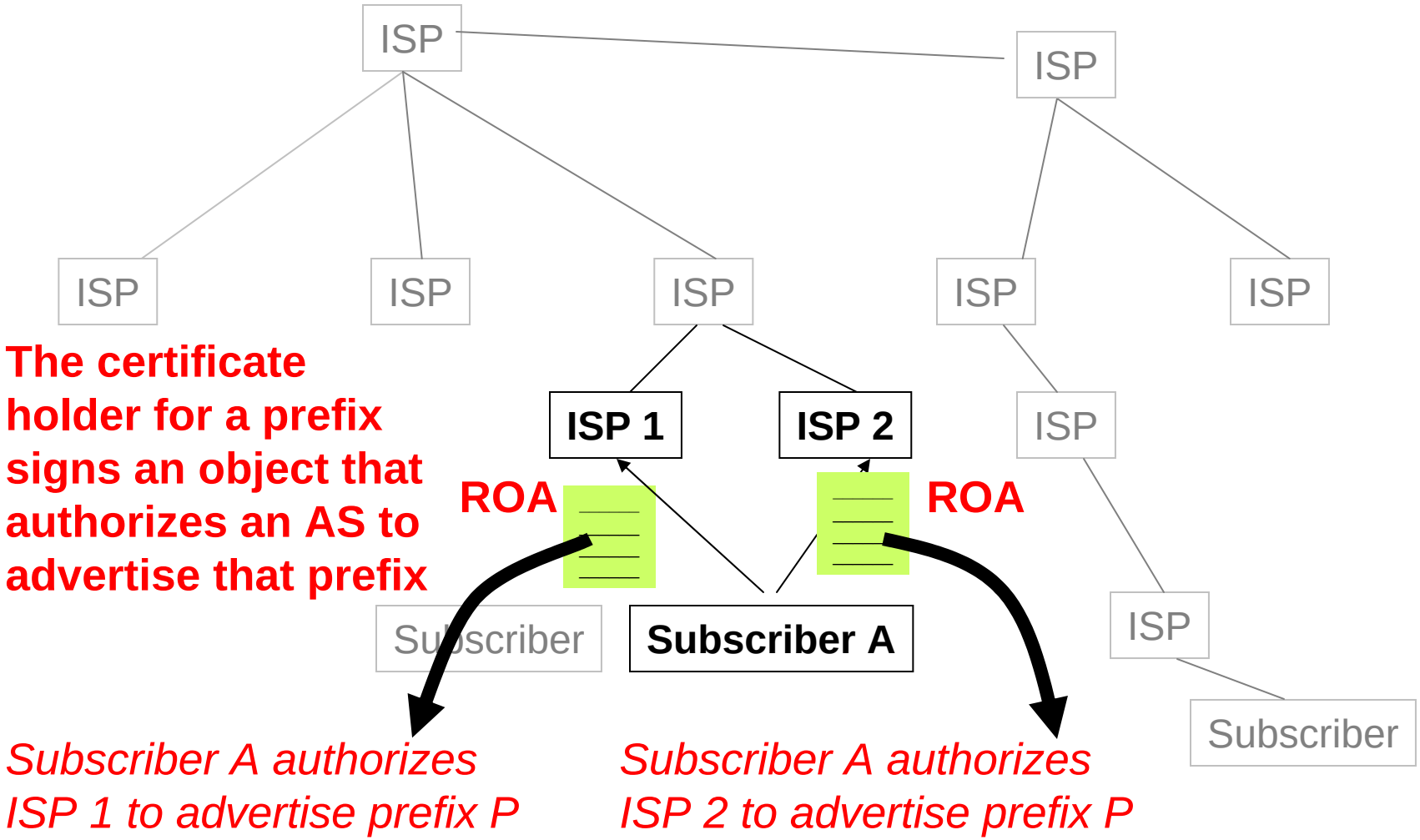
SPARTA, Inc

sandy@sparta.com, sandy@tislabs.com

Resource PKI



And Then the Routing Part



Use with existing prefix filter generation tools

- The ROA sounds a lot like an RPSL route object.
- Idea: generate a database of route objects from a database of ROAs; feed into existing tools
- For: fits will current operational filter generation
- Against: introduces a (fixable) vulnerability, depending on what the tools do with an empty database
  - No route objects -> no filter: if you haven't created route objects on your own, some else's ROA makes a peer produce a single prefix filter (all your other prefixes blocked)
  - No route objects -> empty filter: no big problem; the peer produces a single prefix filter instead
- Q: How would this work with your own filter generating process? (even if you don't have one)

What's the root?

- IANA may or may not be ready, willing, able, authorized to be the trust anchor the RPKI.
- The architecture jumps through hoops to provide for a (small) forest of trust anchors.
- For one root: for multiple roots, operators will need to assign authorization to each trust anchor. Every couple of months. (Sound familiar to bogon filters? It's the same problem.)
- Against one root:
  - we don't know what IANA is going to do, so we have to be prepared
  - relying parties always have the right/ability to choose their trust anchors and assign authorization to trust anchors.
- How do operators feel about this issue? Need to let us know and also speak up in the RIR communities as well. Maybe ICANN.

Validating BGP Updates during partial deployment

- Need to be able to choose between BGP route that has a ROA and one that does not.
- No problem in full deployment - un-ROA'd routes are trash. But in partial deployment? Which announcements are SUPPOSED to have ROAs?
- One idea: announce a BOA - Defined as "believe no routes for this" - but trumped by a ROA, so more like "believe no routes but those with ROAs"
- Another idea: the ROA set is exclusionary (like filters) – if there are any ROAs for a route, un-ROA'd routes are out. Problem: how to prevent hijacks if you are not announcing this prefix (no ROA)
  - internal infrastructure; exchange points; allocated by not yet used prefixes?
  - so if you are not going to announce a prefix, just create a ROA for a fictitious AS.
- Various ideas of how each idea would relate to choosing between a route to a prefix that had a ROA and a route that did not.
- Q: Suppose the operational use required that you sign ROAs for all announced routes. Not just some. OK?

Validating BGP Updates during incomplete usage

- Suppose
  - you get an RPKI certificate with your prefix, and you do ROAs for your announcements.
  - you allocate a sub-prefix to a customer who is multi-homed and they can not do ROAs yet.
  - How do other operators tell your customer's legitimate routes from a more specific prefix hijacking of your prefix?
- Q: Suppose the ISP was expected to generate routes for its clueless but multi-homed customers. (Or run a service on behalf of its customers) OK? What about your clueful grandchildren - your clueless customer's clueful customers?

What you can do

- Get involved in the discussion, that's the only way to make sure the answers come out friendly to your sanity.