Securing the Routing Infrastructure - Status and Request for Comments

Sandra Murphy Sparta, Inc

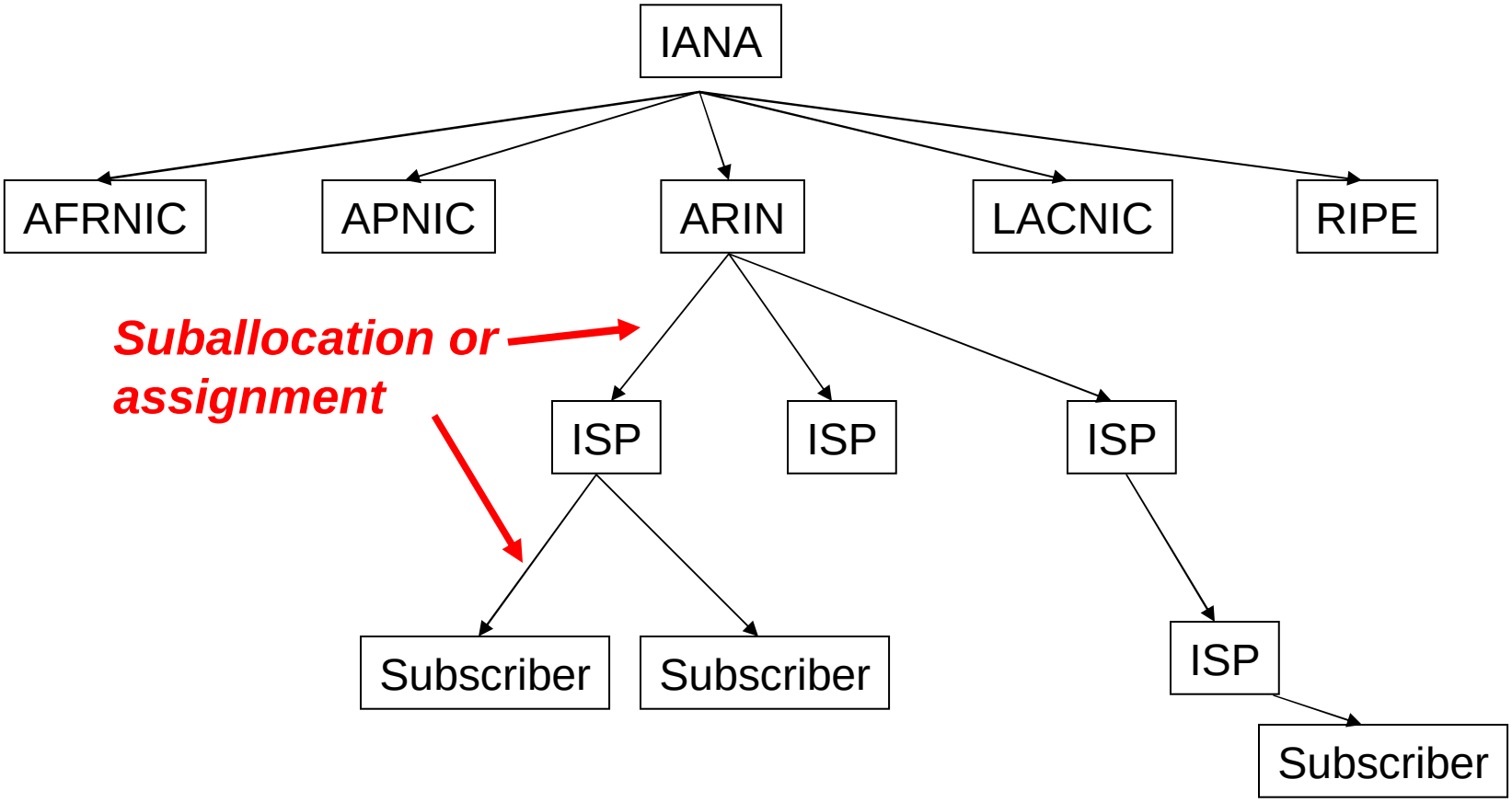
Sandra.murphy@sparta.com

(funding provided by DHS S&T)

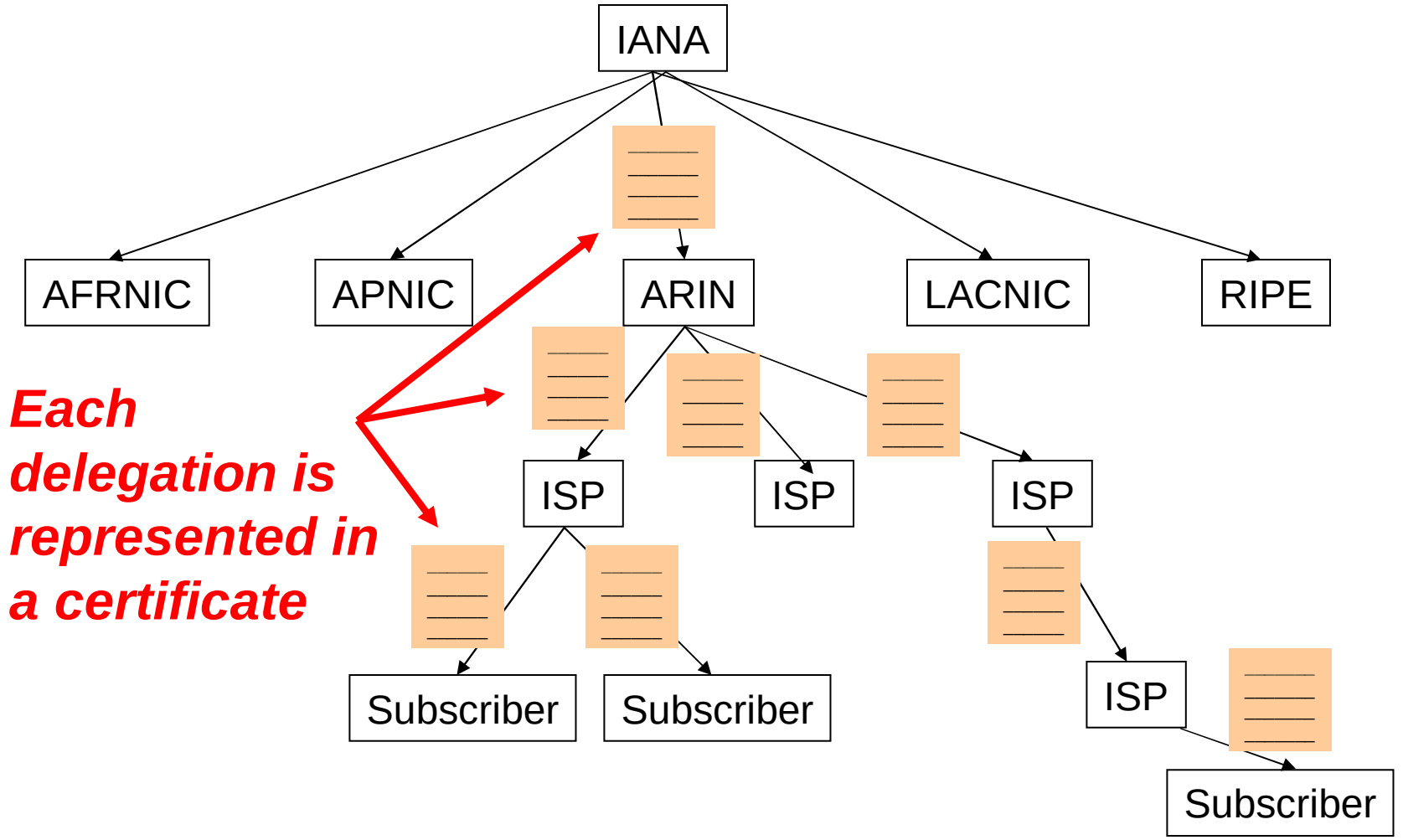
Securing Who Holds What Prefixes

- A certificate structure has been presented at various meetings in the last year or so: NANOG, ARIN, RIPE, APRICOT, …
  - NANOG 36 Feb 2006: What I Want for Eid ul-Fitr, An Operational ISP & RIR PKI
  - APRICOT Mar 2006: A PKI to Support Improved Internet Routing Security
  - ARIN XVII April 2006: X.509 Resource and Routing Certificate Panel
  - RIPE 52 Apr 2006: A PKI for IP Address Space and AS Numbers
  - NANOG 38 Oct 2006: Serious Progress on X.509 Certification of RIR Resource Allocations
  - RIPE 53 Oct 2006: Using Resource Certificates - A Progress Report on the Trial of Resource Certification

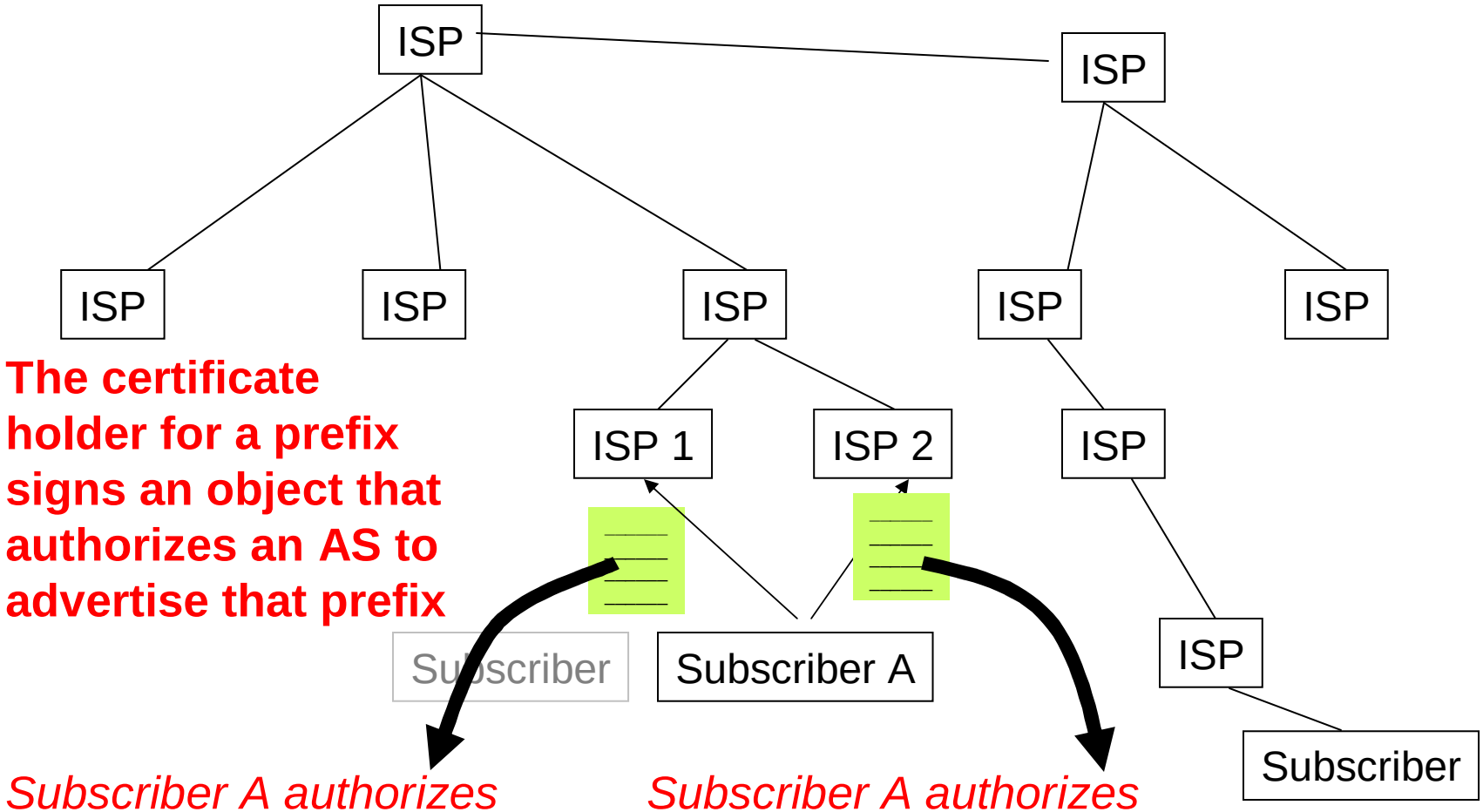
Address Delegation



Resource PKI



And Then the Routing Part



The certificate holder for a prefix signs an object that authorizes an AS to advertise that prefix

Subscriber A authorizes ISP 1 to advertise prefix P

Subscriber A authorizes ISP 2 to advertise prefix P

The IETF SIDR Working Group

- Chartered to work on the resource certificate architecture and a secure route origination mechanism (Route Origination Authority: ROA)
- Resource certificate Internet-Draft
  A Profile for X.509 PKIX Resource Certificates
  http://smakd.potaroo.net/ietf/all-ids/draft-ietf-sidr-res-certs-02.txt
- ROA to be a draft by March IETF
- Architecture to be a draft by March IETF
  - There have been lots of presentation; no draft

SIDR Discussions

- A wrinkle in signing ROAs
- Generally considered unwise to use a CA certificate to sign anything but another certificate
- So don’t use the address certificate to sign the ROA
  - Instead, for each advertised prefix, create another non-CA certificate (an EndEntity certificate) and use THAT to sign the ROA
  - Revoking the ROA is accomplished by revoking the EE certificate

SIDR Discussions

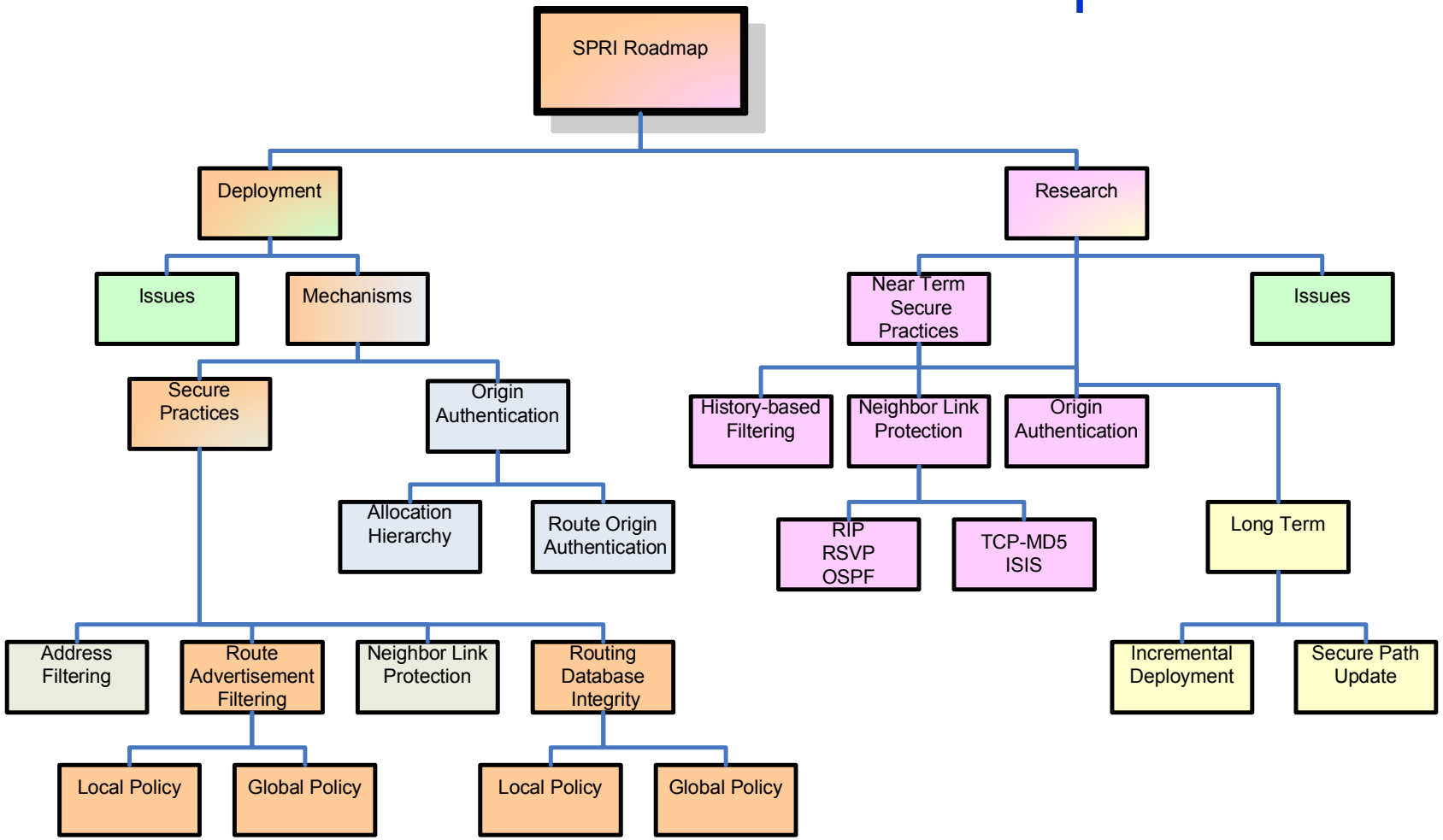
- ROA content
  - Trying to keep it simple
  - Authorizes one ISP to advertise a prefix
    - If you are multi-homed, use multiple ROAs
    - Q: if the ISP has more than one AS, list them or make a list of ROAs
  - Prefix list
    - Since there is one EE certificate for each advertised prefix, don't actually need to put the prefix in the ROA

SIDR Discussions

At the last IETF meeting we discussed:

- Adopt RIPE authorization model?
  - both the prefix holder and the advertising AS must authorize the route advertisement (RFC 2725)
  - Working group decided against this
- Route validity
  - Exact match: ROA prefix must exactly match advertised NLRI
  - Covering match: ROA prefix must cover the advertised NLRI
  - No consensus in the meeting

Secure Protocols for the Routing Infrastructure - Roadmap



For the full document, see http://www.cyber.st.dhs.gov/spri.html

Please Participate

- You can see the sidr working group charter and mailing list archive at: http://www.ietf.org/html.charters/sidr-charter.html
- The mailing list is
  - General Discussion: sidr@ietf.org
    To Subscribe: sidr-request@ietf.org
    In Body: (un)subscribe