RPKI Gray Area: Inheritance?

IETF 83, SIDR WG

Contributors:

Andrew Chi (BBN), Rob Austein (DRL),

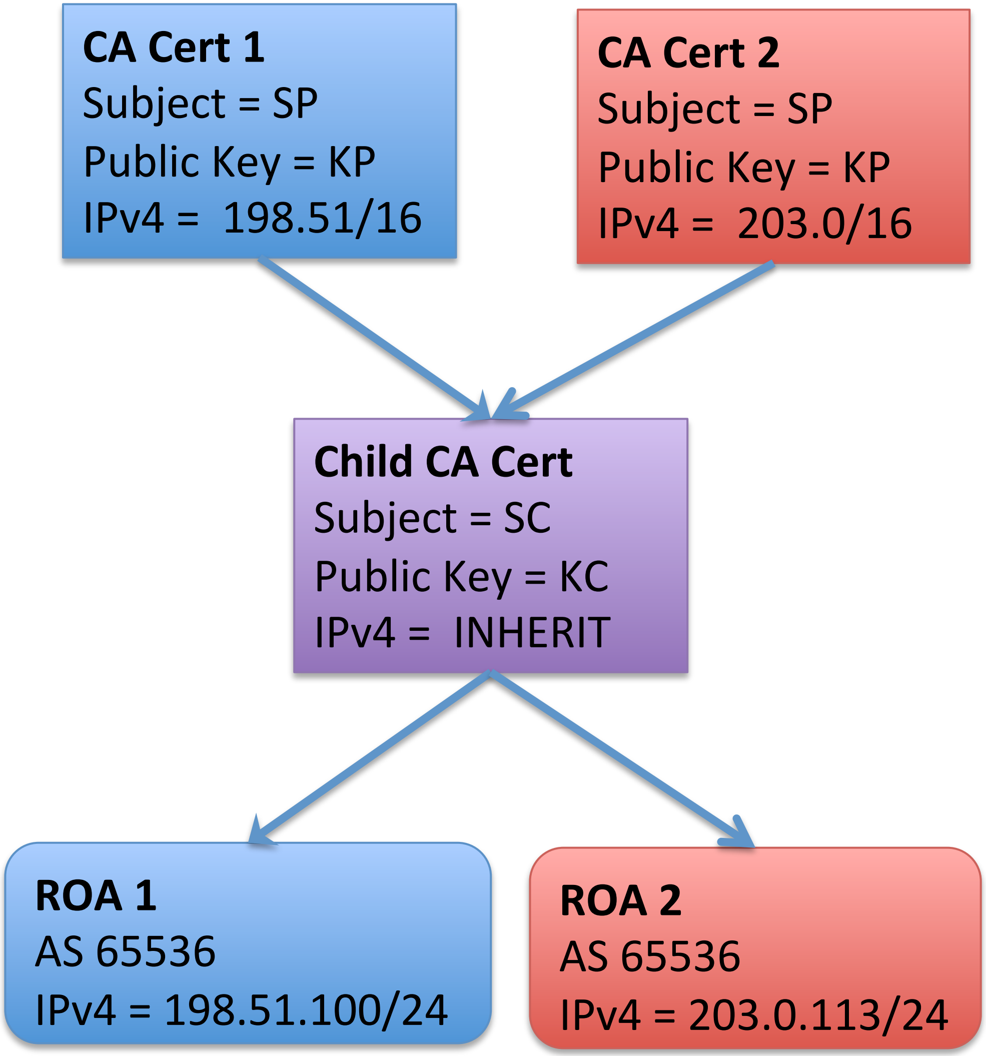
Tim Bruijnzeels and Miklos Juhasz (RIPE NCC)

Gray Areas Discussions at IETF 83

- 3/26 and 3/27: RPKI validator implementers hashed through some “gray areas.” Topics included:
  - Multiple access description URIs (e.g. SIA, CRLDP), unknown extensions, OID discrepancies, inheritance, rsync download limits, manual blacklisting, key rollover, manifest errors, what to do if parts of RPKI are temporarily unavailable.
  - A couple of errata already submitted.
- Summary will be emailed to SIDR list; gray areas should be captured in a doc eventually.

- We implementers want clarification on inheritance.

Ambiguous Inheritance



CA Cert 1
Subject = SP
Public Key = KP
IPv4 = 198.51/16

CA Cert 2
Subject = SP
Public Key = KP
IPv4 = 203.0/16

Child CA Cert
Subject = SC
Public Key = KC
IPv4 = INHERIT

ROA 1
AS 65536
IPv4 = 198.51.100/24

ROA 2
AS 65536
IPv4 = 203.0.113/24

- RFC 3779 “Inherit” in CA certificates permits this.
    - Left ROA is valid via left parent only. Right ROA is valid via right parent only.
    - Validators must remember all possible “inherited” resources (not the union) in order to avoid multiplicative path explosion.
    - Note: Any CA in the RPKI can create an equivalent to CA Cert 2 (though not ROA 2).

- ROA EE certs are already forbidden to use “Inherit”, so no problem there.

Opinions?

- What are the your “inherit” use cases?

- Can we forbid inheritance in CA certs except where it’s absolutely critical?
- Or: Did we miss a validation approach that is less confusing?
- Or: “Tough” ☺