“RPKI Validation Reconsidered” Revisted

Sandra Murphy

Multiple motivations?

- Transfers?

  "The question considered here is: Is there an alternate definition of RPKI certificate validity that could remove the requirement for such careful orchestration of certification actions across the RPKI to support resource transfers?" (draft-huston-rpki-validation)

- Higher ups deliberate actions?

  "The problem is that when a CA is compelled to remove a resource from a certificate (be it a court order, pressure from some agency, …" (draft-huston-rpki-validation)

- Higher-ups making mistakes?

  "… or fat fingers" (draft-huston-rpki-validation)

Solution

- New encompassing rule: Do the resources in each ancestor certificate in the tree encompass the given resource set
  - So if one cert's resources are reclaimed, those resources that are retained can still be valid
  - Each cert has new locally constructed structure – which of the cert's resources are valid

My Opinion on Motivations

- Transfers?
  - *Transferee has control over timing here – request split of cert, etc.*
- Higher ups deliberate actions?
  - *Higher up has control over timing here - repair links that would be affected*
- Higher-ups making mistakes?
  - *No control over timing*

My Own Opinion on Solution

- Certs have always been said to certify allocations – this removes that tie.
- A CA could now issue cert for resources it has not yet been allocated:

  "each CA can issue a certificate with an augmented resource set that includes the resource being transferred without particular regard to the timing of similar actions by the other superior or subordinate registry CAs."

  - That's **ANY** resources it has not been allocated.
  - But they won't be judged "valid".
- Same applies to continuing to issue certs for resources that have been recalimed.
- How does this validation apply to other signed objects not resource bearing – ghostbusters for example?

Now Discuss

- What is the problem here?
  - Is it important?
  - Is it something the IETF can address?
- If so, is draft-huston-rpki-validation a/the solution?