Deploying Validation Reconsidered

George Michaelson ggm@apnic.net
Tim Bruijnzeels tim@opennetlabs.nl
Deploying Validation Reconsidered

George Michaelson  ggm@apnic.net
Tim Bruijnzeels  tim@opennetlabs.nl

“three or four slides smaller than last time”
Problem Statement

• Deployment requires three things in coordination [*]
  1. Available code to sign and validate objects under the new OID
  2. Agreement to move to the new model by relying parties and signers
  3. A decision about how to move
     – Either it’s like a flag-day as in RFC6916
     – Or it’s a mixed-mode operation in one tree

[*] In no implied order
Available code to sign and verify

• Code changes for signers are minimal
  – If it’s a flag-day. Its “one line” to move to the new OID in the code which mints certificates with the private key
  – If it’s mixed-mode, it’s the option to choose the OID, and UI or protocol changes to support specification of which OID is to be used in the specific moment of signing

• Code changes for verifiers are less easy
  – Can minimally change to permit new OID, for ‘fully covered’ case
    • Change to handle oversign properly requires more work
      – Parse out and hold the valids, flag the overclaim, move on
      – Transition moments through intermediate objects. New data structures…
Agreement to move to the new model by relying parties and signers

• There has been no active engagement to discuss a timeline.

• We (the RIR) wish to propose some future date, TBD, as a "flag day" to give one year to prepare to migrate

• We want to go into the *-NOG and other forums to seek consensus to move from operators and related parties
What kind of deployment?

• “there can only be one” (OID) demands flag day
  – Analogous to RFC6916
  – All or nothing, but simple
  – Transition happens through a staged window of dual state

• “we can mix it up”
  – Operate mixed-mode, signing CA determines setting over child
  – RIRs seek flag-day to release TAL which bear the new OID
  – Still requires acceptance of the new OID to deploy TAL so still carries the need for consensus in code and userbase
Tri-partite deployment deadlock

• Can’t move without code

• Can’t move without consent/agreement by RPs and Cas

• Can’t deploy new TAL without either of the above
It doesn’t get easier by waiting

• Present at *NOG to seek consensus to deploy at a TBD

• As it stands, we’re talking a moment of change for < 500 entities (more downstream affected parties, IP coverage not measured)
  – It’s already a distributed problem

• Flag day move to new OID is logistically simpler
  – Hack: simply recognize but reject overclaim == current model
  – In either case, deployment of TAL with new OID would be fatal to RP if validators don’t implement
Where to from here?

• Seeking WG adoption:
  – Pick a method
  – Discuss a timeline

• Gauge Operations community engagement at NOG
  – Assuming we get traction/consensus to proceed in the operations community…

• Define the TBD date
  – Coordinate with s/w developers to support new OID