Deploying Validation Reconsidered

George Michaelson ggm@apnic.net
Tim Bruijnzeels tim@opennetlabs.nl
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…
Available code (continued)

• None of the deployed CA/Signers appears ready yet
  – but its trivial
• (I believe) RIPE Validator team has at least discussed modified validation and may have code in test
• RPSTIR, Dragon Research not believed to have code
• We have an explicit dependency in the APNIC region on dragon s/w
  – 3-4 NIR using Dragon for signing (JPNIC, CNNIC in deployment or near, TWNIC, IDNIC in internal test)
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 July 2019 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
Who is “in the system” as RPs?

- 178 unique ASNs over 302 IP addresses in rsync
- 39 unique ASNs over 65 IP addresses in rrdp
  - Of which half are demonstrably RIPE code (User Agent Strings)
  - All of whom also appear in Rsync logs, fetching CA under TAL
- Allowing for “don’t upgrade”, possibly more using RIPE code but certainly not most
- The majority of seen clients are probably using Dragon Research or RPSTIR
<table>
<thead>
<tr>
<th>CC</th>
<th>Country</th>
<th>CC</th>
<th>Country</th>
<th>CC</th>
<th>Country</th>
<th>CC</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>38</td>
<td>US</td>
<td>23</td>
<td>DE</td>
<td>14</td>
<td>RU</td>
<td>12</td>
<td>NL</td>
</tr>
<tr>
<td>11</td>
<td>JP</td>
<td>9</td>
<td>FR</td>
<td>6</td>
<td>CN</td>
<td>5</td>
<td>ZA</td>
</tr>
<tr>
<td>5</td>
<td>GB</td>
<td>5</td>
<td>CH</td>
<td>3</td>
<td>CZ</td>
<td>3</td>
<td>CA</td>
</tr>
<tr>
<td>2</td>
<td>UA</td>
<td>2</td>
<td>TH</td>
<td>2</td>
<td>SE</td>
<td>2</td>
<td>PT</td>
</tr>
<tr>
<td>2</td>
<td>NZ</td>
<td>2</td>
<td>NO</td>
<td>2</td>
<td>MU</td>
<td>2</td>
<td>LU</td>
</tr>
<tr>
<td>2</td>
<td>IT</td>
<td>2</td>
<td>HU</td>
<td>2</td>
<td>GR</td>
<td>2</td>
<td>BG</td>
</tr>
<tr>
<td>2</td>
<td>AU</td>
<td>2</td>
<td>AT</td>
<td>1</td>
<td>ZZ</td>
<td>1</td>
<td>VN</td>
</tr>
<tr>
<td>1</td>
<td>UY</td>
<td>1</td>
<td>TW</td>
<td>1</td>
<td>SK</td>
<td>1</td>
<td>SI</td>
</tr>
<tr>
<td>1</td>
<td>RS</td>
<td>1</td>
<td>RO</td>
<td>1</td>
<td>QA</td>
<td>1</td>
<td>PL</td>
</tr>
<tr>
<td>1</td>
<td>MY</td>
<td>1</td>
<td>MV</td>
<td>1</td>
<td>MN</td>
<td>1</td>
<td>MG</td>
</tr>
<tr>
<td>1</td>
<td>LV</td>
<td>1</td>
<td>KR</td>
<td>1</td>
<td>ID</td>
<td>1</td>
<td>EC</td>
</tr>
<tr>
<td>1</td>
<td>CY</td>
<td>1</td>
<td>CR</td>
<td>1</td>
<td>BT</td>
<td>1</td>
<td>BR</td>
</tr>
<tr>
<td>1</td>
<td>BE</td>
<td>1</td>
<td>AR</td>
<td>1</td>
<td>AM</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
It doesn’t get easier by waiting

• Present at *NOG to seek consensus to deploy July 2019

• 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