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

	CC		CC		CC		CC
38	US	23	DE	14	RU	12	NL
11	JP	9	FR	6	CN	5	ZA
5	GB	5	CH	3	CZ	3	CA
2	UA	2	TH	2	SE	2	PT
2	NZ	2	NO	2	MU	2	LU
2	IT	2	HU	2	GR	2	BG
2	AU	2	AT	1	ZZ	1	VN
1	UY	1	TW	1	SK	1	SI
1	RS	1	RO	1	QA	1	PL
1	MY	1	MV	1	MN	1	MG
1	LV	1	KR	1	ID	1	EC
1	CY	1	CR	1	BT	1	BR
1	BE	1	AR	1	AM		

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