draft-ietf-sidrops-manifest-numbers-02

●●●

Tom Harrison (tomh@apnic.net)
George Michaelson (ggm@apnic.net)
Job Snijders (job@fastly.com)
IETF 121 SIDROPS Working Group

What is this about?

- Manifests include a field called **`manifestNumber`**
- Existing documents require that new manifests have larger **`manifestNumber`** values than previous manifests
- **`manifestNumber`** has a maximum value (largest 160-bit signed integer)
- If that value is reached, CA is unusable, at least until the manifest expires
  - Not great for standard CA, but they can roll over, at least
  - But TAs don't have that option
- So: very low chance of occurring, but serious problem if it does

How should RPs handle this?

- If the CA changes the manifest filename, then reset the stored **`manifestNumber`** for the CA
  - Simple, should be easy to implement
  - Already implemented in rpki-client

Changes since IETF 119

- Document that the maximum value is largest 160-bit signed (rather than unsigned) integer
- RPs must check object SIAs against RRDP publication URLs
- Handling for CAs with multiple manifest SIAs
- Note that maximum-value problem does not affect **`thisUpdate`**
- Note that CRL numbers are being dealt with separately

Why not just deprecate `manifestNumber`?

- It is useful for diagnostics
  - Absence of contiguous sequence in RRDP will generally indicate underlying CA problems (see Job's last mail)
- Regression may indicate problems like invalid restore from backup
  - Generally preferable in that case to use existing cached state
- Already implemented
  - If checking is deprecated, some CAs will continue with current practice, while some will not – potentially confusing
- Proposed fix is not costly
  - In particular, there is no additional need to implement serial number arithmetic

RP support for 9286 and this draft

	validador FORT			
Manifest number reuse	Accepted	Accepted	Rejected	Rejected
Manifest number regression	Accepted	Accepted	Rejected	Rejected
Manifest number of max 160-bit signed	Accepted	Accepted	Accepted	Accepted
Manifest number > max 160-bit signed	Rejected	Accepted	Rejected	Rejected
Reset on manifest filename change	N/A	N/A	Yes	Yes
Location mismatch check	No	No	No	Yes

https://github.com/APNIC-net/rpki-mft-number-demo

Next steps

- WGLC?