Algorithm Agility Procedure for RPKI: WGLC Issues & Fixes

Steve Kent

BBN Technologies

Algorithm Migration Documents

- The underlying assumption about what will motivate an algorithm transition was not clearly described.
- Revised Section 2 text

The algorithm transition process described in this document is not intended to support an emergency transition of the sort that might be required by the discovery of some serious algorithmic vulnerability. Use of standard algorithms that have very widespread adoption and that have undergone extensive analysis prior to adoption make the likelihood of an emergency transition very, very small.

Policy OID and Algorithm Transition

- The algorithm transition document did not make clear whether the policy OID for RPKI certificates (as specified in the CP) would change when the RPKI algorithms document was revised
- Added Section 2 text:

The CP will not change as a side effect of algorithm transition (and thus the policy OID in RPKI certificates will not change.)

Transition Timetable

- It was suggested that the timetable for the transition phases should be a produced by organizations that represent the CAs and RPs, rather than being an IETF-authored document
- Revised Section 2 text:

An additional document, the algorithm transition timetable, will be published (as a BCP?) to define the timeline for the algorithm suite transition. It will defines dates for the phase transitions, consistent with the descriptions provided in Section 4. It is RECOMMENDED that the timeline document be developed by the entities that act as CAs, RPs, and repository operators in the RPKI, e.g., IANA, Internet Registries, and network operators. It is also RECOMMENDED that the timeline document describe procedures to track the progress of the transition and to amend the timeline, e.g., if problems arise in implementing later phases of the transition.

Revising the Timetable

- It was requested that the document be augmented to discuss what types of events might cause the timetable to be revised, and what the impact would be at each phase
- Text is being added to each phase description to address this request (Sections 4.3-4.8)
- For most phases, there is no need for a “rollback” if the phase is postponed.
- Since the timetable document will not be written until there is a need to initiate algorithm transition, this text is best placed in the current document.

Is EOL Really a Return to Phase 0?

- The current process defines EOL for the old algorithm suite as a return to Phase 0
- But, Phase 0 includes a definition of the next algorithm suite!
- So, we probably need to revise Section 4.8 to say this differently (and update the figure on page 9)

Top-down vs. Laissez Faire

- The algorithm agility document proposes a global, top-down algorithm transition process
- The top-down aspect was adopted by the WG after the Maastricht meeting, where we acknowledged the exponential growth of the repository system that can result from a laissez faire transition approach
- Also, a CA cannot unilaterally elect to change its certificate to a new algorithm, because the parent CA must be able to perform PoP using the new algorithm.

Global vs. Local Transition Process

- The need for the process to be global has been questioned
- The process is defined as a global one to make life easier for RPs and CAs
- If there are no global dates for transition phases
  - CAs don’t know when they MUST be prepared to issue certificates under a new algorithm suite, generate signed products under the new suite, and when they MAY cease support of the old suite
  - RPs don’t know when they MAY request certificates under the new suite, MAY generate and publish objects, and when the MUST be able to process objects from CAs