Status Update for Algorithm Transition for the RPKI (draft-ietf-sidr-algorithm-agility)

Steve Kent

Roque Gagliano

Sean Turner

Algorithm Transition Document

- SIDR agreed to adopt this as a WG item, and a new version appeared in late February
- Target is a standards track RFC from SIDR
- The document describes
  - What CAs have to do to effect algorithm transition
  - What RPs can expect during algorithm transition
  - How transition interacts with repository structure
  - How algorithm transition and key rollover interact

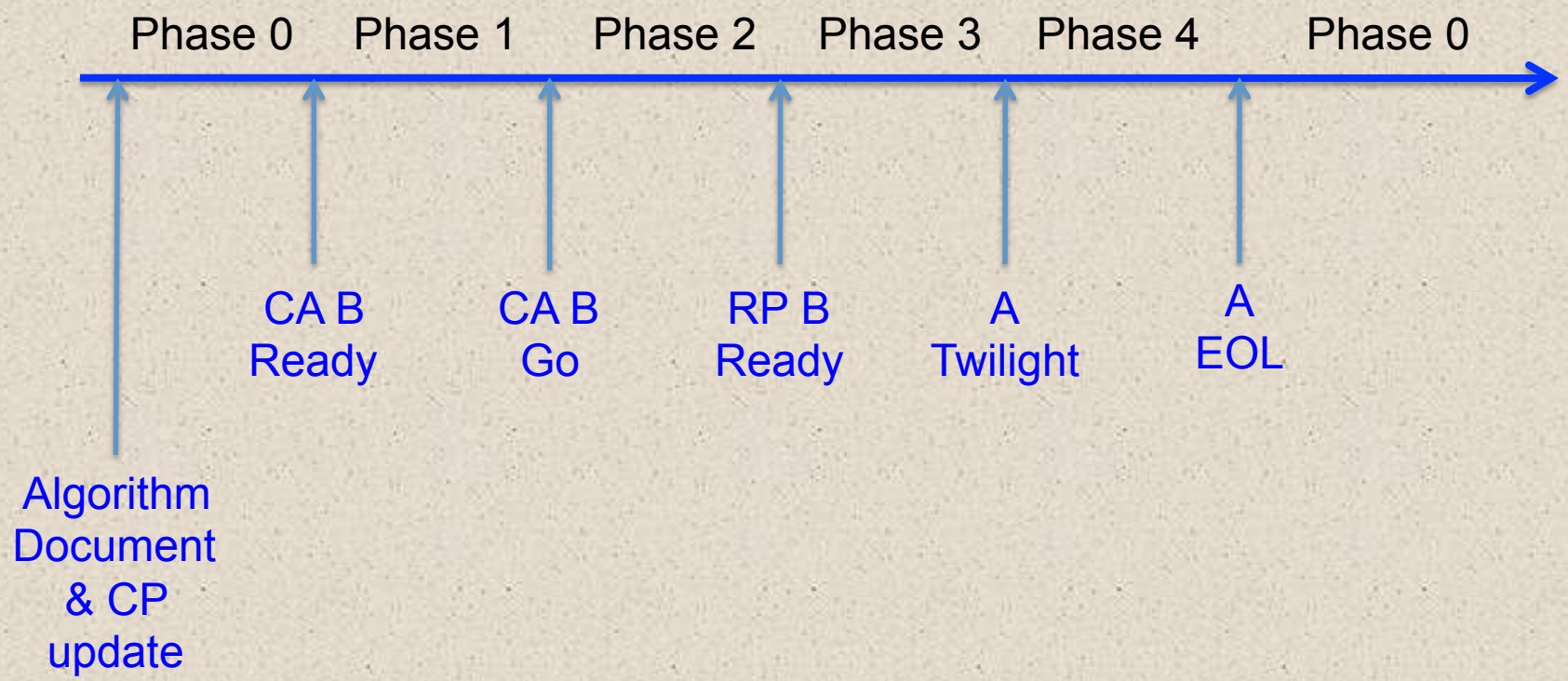
Changes from the Individual Submission

- Adopted top-down transition model
- The document now describes
  - Multi-algorithm support in the provisioning protocol
  - Dealing with multiple instances of signed products
  - Use of independent publication points
  - Key rollover is independent per algorithm suite
  - Parallel certificates MUST be revoked together
- Added Security Considerations & Acknowledgements sections

Terminology

- Algorithm A - the current signature and hash algorithm suite
- Algorithm B - the next signature and hash algorithm suite

CA & RP Transition Phases



Algorithm Transition Milestones (1/2)

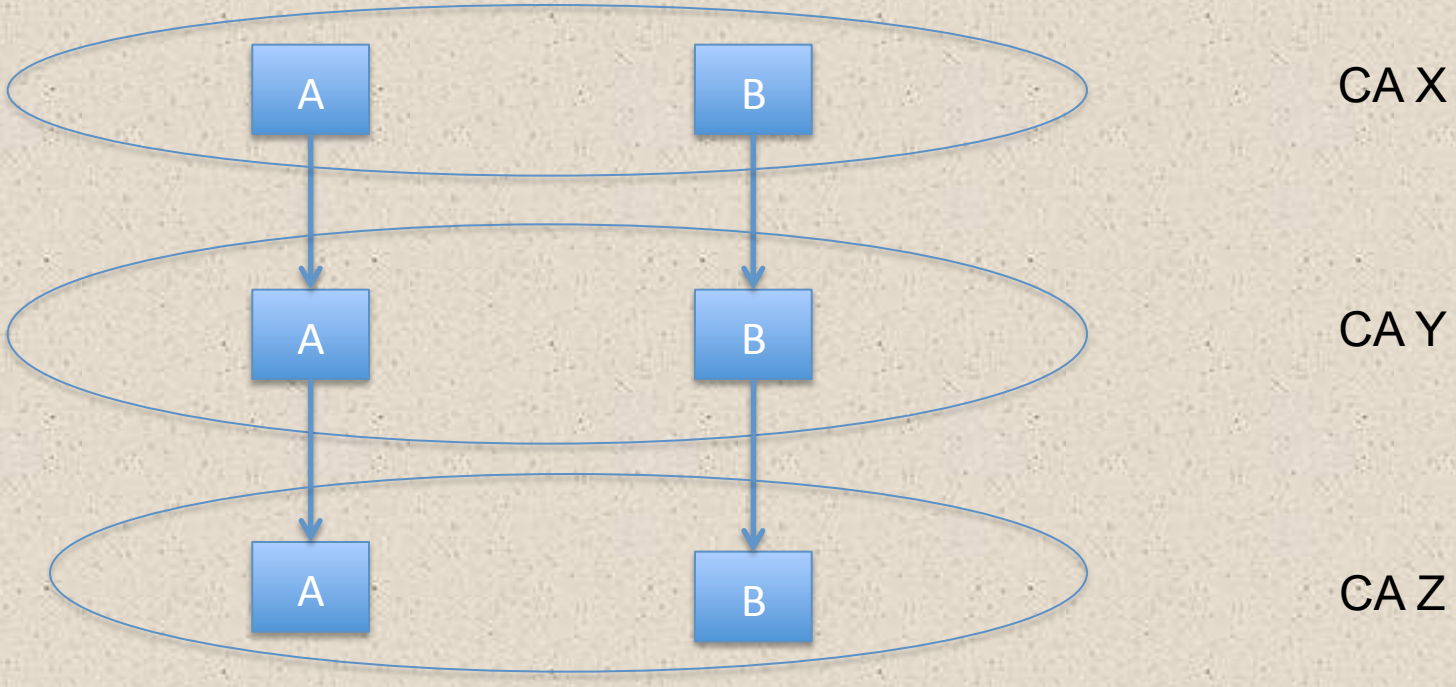
- Steady state (using algorithm A)
- Update algorithm specification and CP
- CA Algorithm B Ready – all CAs are ready to process a certificate request for a certificate containing an Algorithm B key, signed under Algorithm B
- CA Algorithm B Go – all CAs reissue all signed products under Algorithm B (and continue issuing under Algorithm A)

Algorithm Transition Milestones (2/2)

- RP Ready Algorithm B – all RPs are ready to process signed products using Algorithm B
- Twilight Algorithm A – CAs MAY stop issuing signed products using Algorithm A, and RPs MAY cease validating signed products under Algorithm A
- EOL Algorithm A – CAs no longer issue signed products using Algorithm A, and RPs reject any signed product under Algorithm A

Top-down Transition Model

CA X's parent has to issue an Algorithm B certificate to CA X before that CA can issue an Algorithm B certificate to CA Y



If each CA issues certificates that use the same algorithm for certificate signing and for the key in the certificate, then directory growth is at most 2X.

Repository Management

- The transition process requires CAs to publish signed products under both algorithms
- During "CA Algorithm B Ready" there may be only a few products (CA certificates) under Algorithm B, so the duplication is not complete
- By "CA Algorithm B Go" a full, duplicate product set exists, 2X repository size
- Using separate publication points makes life simpler

Relying Parties

- This design provides RPs with signed products under the current and new algorithms for a while, because we assume that it will take a while for ALL RPs to be able to make the transition
- This imposes a burden on CAs to maintain parallel signed product sets from “CA Algorithm B Go” until “Algorithm A Twilight”
- If an RP fetches both product sets, and either set is OK, then that’s good enough!

Observations

- This is still a new document, and thus needs review and comments from the WG
- It is only a 25 page document, but the process is complex, so it calls for careful reading
- We have had almost no comments from the broad WG population so far

Please read and provide feedback!