BGPSEC Router Certificate Rollover

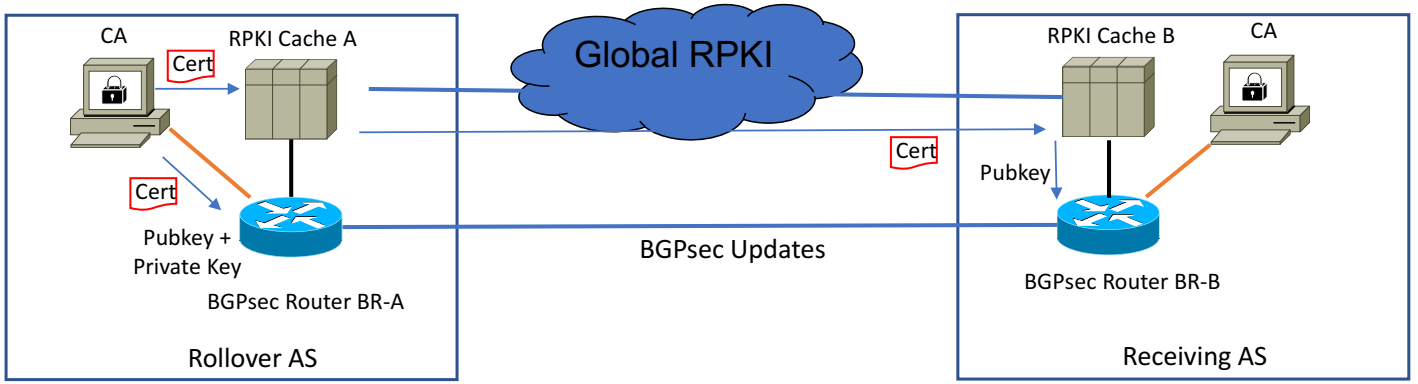
draft-ietf-sidrops-bgpsec-rollover-00

Brian Weis

Roque Gagliano

Keyur Patel

Overview of Router Keying through the RPKI



- A BGPsec Router (e.g., BR-A) obtains a keypair (public key + private key), receives a certificate from its local CA.
- It's RPKI Cache forwards the certificate (containing it public key) through the RPKI, which is validated by the global RPKI Cache (e.g., including RPKI Server B)
- The public key from the certificate is forwarded to other BGPsec routers (e.g., BR-B) for verification of BGPsec Updates (e.g., signed by BR-A)

  It is critical that BR-B receive the Pubkey from BR-A *before* it receives BGPsec Updates validated with that Pubkey!

  Initial distribution of BGPsec Router certificates is not likely to be a problem, but when the BGPsec Router keys are replaced synchronization between certificate distribution and usage of the new keypair for signing BGPsec Updates is necessary.

Certificate-only rollover events

- Sometimes the BGPsec Router certificates need to be replaced, but the pubkey in the certificate is still valid. For example:
  - Expiration date (NotValidAfter) requires a replacement certificate ("BGPSEC scheduled rollover")
  - Something in the certificate (such as the AS Resource Identifier or Subject) changes. ("BGPSEC certificate fields changes")
- If the AS security policy allows it and key exposure is not suspected, then the keypair used by the router need not be replaced.
  - In this case, the new certificate is propagated through the RPKI but the peer BGPsec routers do not need to be aware of the rollover.
  - I.e,. the peer BGPsec router RPKI state remains stable regardless of a certificate rollover
  - However, if the original certificate is near expiration, the same process is necessary to ensure that its replacement certificate is distributed through the RPKI before it expires.

Rollover events: New BGPsec router certificate & keypair

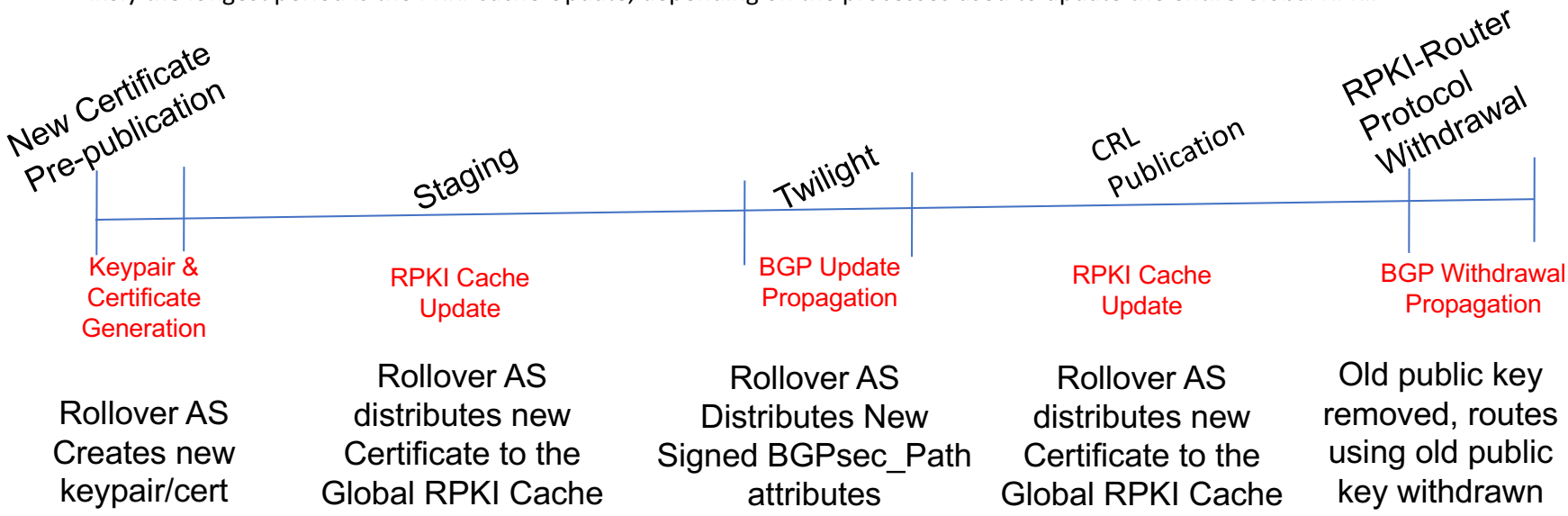
- The previously mentioned rollover events may cause a BGPsec router keypair rollover. Other rollover events should require distribution of a new BGPsec router keypair.
  - A compromised BGPsec router secret key requires the replacement of a BGPSEC certificate (“BGPSEC emergency rollover”)
  - An AS may determine stale BGPsec_Path attributes continue to be propagated (e.g., the latest origin signature on a BGPsec_Path is being withheld somewhere on the path) (“BGPSEC signature replay protection”)
- A rollover event may also require an updated Certificate Revocation List (CRL), which must be considered in the rollover event.

Steps in the Rollover

1. New Certificate Pre-publication
   - The Rollover AS generates a new keypair (if needed) and obtains a new certificate for the BGPsec router
   - If the keypair is generated elsewhere, the new keypair is also positioned onto the BGPsec router
2. Staging Period
   - The Rollover AS makes the new certificate available to the RPKI global repository. The new certificate is propagated and verified by RPKI Caches
   - When a new keypair is distributed, each AS using the global RPKI-Cache will add the new key to its BGPsec routers
3. Twilight
   - Rollover AS BGPsec Routers begin using new keys to sign BGPsec_Path attributes
   - They also must generate new BGPsec_Path attributes for every BGPsec_Path attributes previously signed by the old key (both origin and transit signatures)
4. CRL Publication (optional)
   - The Rollover AS distributes a CRL including the Serial Number of the old certificate. This follows the Twilight step in order to avoid invalidating routing prematurely.
5. RPKI-Router Protocol Withdrawal
   - Each global RPKI-Caches removes the old key from the routers that it manages
   - Routers withdraw any RIB entry that includes an attribute signed with that key

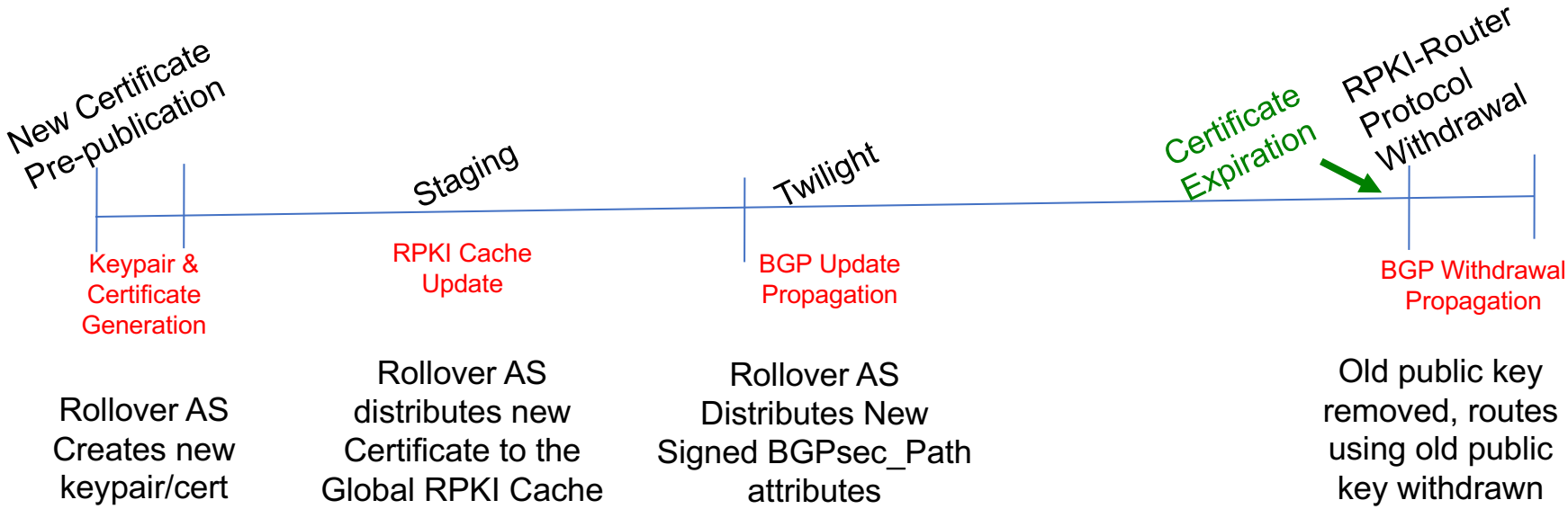
How long is a Rollover Event going to take ?!?

- The duration of the rollover event depends on the number of steps needed, and whether the step is performed with or without human interaction. Each step in the event can be automated, which removes delays waiting on a human (other than starting the process in the first place).
- Likely the longest period is the PRKI Cache Update, depending on the processes used to update the entire Global RPKI.



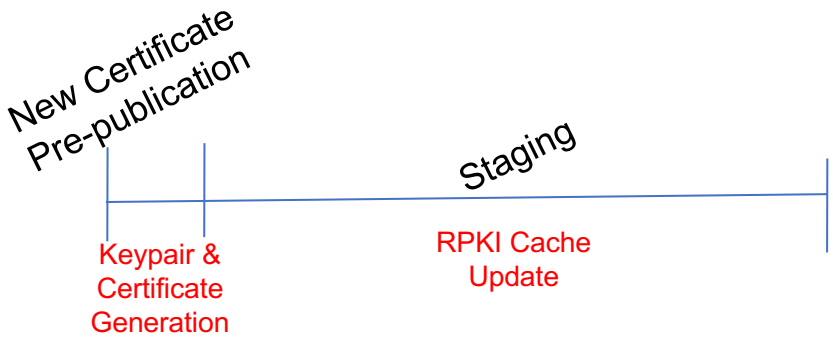
When a CRL publication isn't required

- When a new pubkey is distributed but CRL publication isn't required, then routes signed with the old key may not be withdrawn until the certificate containing that key expires.
- Depending on when the process began, the entire timeline may not be shorter but the method is simpler.



Certificate-only rollover events

- When a new certificate is distributed without changing the public key, then the rollover period effectively ends when the new certificate has been staged.
- There is no change to state on the BGPsec routers.



Proposed Next Steps

- The Internet-Draft is mature (2 individual contributor versions, 6 SIDR versions), and there have not been many recent comments
  - It may be time for a WG last call?
- However, one Informational Reference is an expired Internet-Draft. That would be a good draft to also have published, but should we keep waiting for it?

  [I-D.ietf-sidr-rtr-keying] Bush, R., Turner, S., and K. Patel, "Router Keying for BGPsec", draft-ietf-sidr-rtr-keying-12 (work in progress), June 2016.