BGPSEC Router Key Roll-over

draft-rogaglia-sidr-bgpsec-rollover-00

Roque Gagliano

Keyur Patel

Brian Weis

Goals of this draft

- Key rollover & certificate life-cycle management are necessary topics when developing a PKI
  - RFC 6489 describes a rollover method of RPKI CA keypairs & certificates
  - Rollover of EE certificates is not described, but it is a relatively simple matter of distributing a new EE certificate & ROA before the old one expires
  - However, router BGPSEC adds router keypairs/certificates, and their expiration affects BGP state. It's important to carefully consider and document this process. This is the primary goal of this draft
- We then show that once this rollover method is available that it can be used as a replay mechanism for BGPSEC
  - Preventing replays of updates that do not meet current policy
  - Re-enforcing current policy

Motivations for Router Keypair/ Certificate Rollover

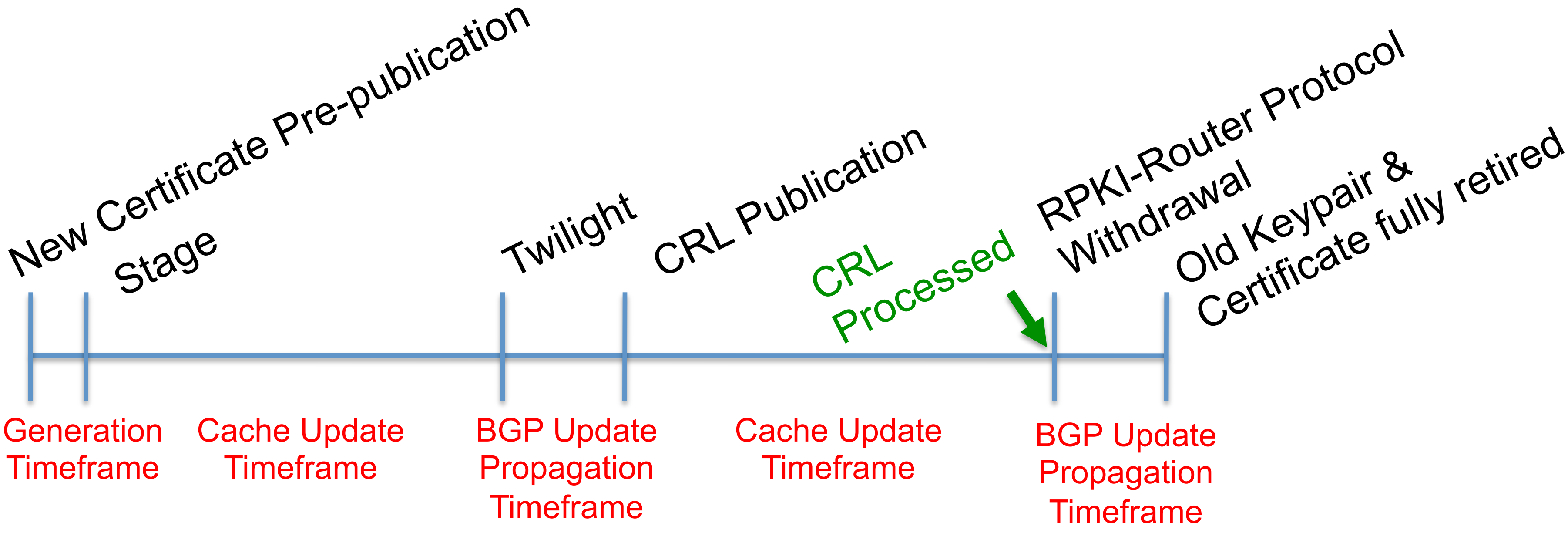
- Scheduled rollover due to AS security policy
  - E.g., periodic renewal of keypairs/certificates because of a certificate lifetime policy
- Changes in certificate fields
  - E.g., a subject name change
- Emergency rollover
  - E.g., due to a router's private key compromise.
  - When all PE routers in the AS share a keypair/ certificate, it is especially important to be prepared to rollover.

Steps in the Rollover

- New Certificate Pre-publication
  - Rollover AS Generates new keypair (optional) and obtains a new certificate for the router(s)
  - If generated elsewhere, keypairs are positioned onto the router(s)
- Stage Period
  - Rollover AS makes the new certificate available to the RPKI global repository and it is propagated to RPKI Caches
  - Each global RPKI-Cache will add the new key to the routers that it manages
- Twilight
  - Rollover AS Routers begin using new keys to sign BGP Updates
  - They also must generate new BGP Updates for every BGP Updates signed by the old key (both origin and transit signatures)
- CRL Publication (optional)
  - If this is an Emergency Rollover, the Rollover AS distributes a CRL including the Serial Number of the old certificate
- 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

Rollover Timeline

(CRL Publication)



New Certificate Pre-publication Stage

Twilight

CRL Publication

CRL Processed

RPKI-Router Protocol Withdrawal

Old Keypair & Certificate fully retired

Generation Timeframe

Cache Update Timeframe

BGP Update Propagation Timeframe

Cache Update Timeframe

BGP Update Propagation Timeframe

Rollover AS Creates new keypair/ Cert

Rollover AS distributes new Certificate to RPKI Caches

Rollover AS Distributes New Signed Updates

Rollover AS Distributes new CRL to RPKI Caches

RPKI Caches remove old public key mapping from routers. Routers withdraw routes using old public key

Operational Requirements

- This process requires nothing different by operations staff over the initial key generation process
  - Generation of a keypair & distribution to all routers using that keypair (if shared)
  - Obtaining a certificate for the keypair & installing it on the local RPKI Cache
  - (Optional) Generating a new CRL & installing it on the local RPKI Cache
- Everything else happens naturally as a function of RPKI operations & router software

Origin vs. Transit Signing

- A transit AS that also originates routes in BGP could benefit from using a unique keypair/certificate for Updates that it originates from Updates that it receives, signs and forwards (i.e., transits)
  - This method reduces the number of Updates that need to be originated and withdrawn if the Origin keypair/ certificate needs to be replaced
  - It may also be possible to choose a longer certificate validity period for the keypair used to sign transit Updates

Rollover without a key change

- When a router certificate rollover happens due to policy (e.g., certificate expiration), it is advisable to issue a certificate with the same key
  - The scope of the rollover is thus restricted to the RPKI Caches
  - There' s no need for routers to issue new Updates or withdraw old Updates, because the router cache has not changed

Other reasons to use the rollover mechanism

- It is necessary to distribute new Updates and Withdrawals as part of the rollover process.
  - These are the same steps needed by any method that changes BGP (e.g., the Expire Time)
  - Can we use a BGPSEC rollover event as a BGPSEC replay protection method?

Replay Protection

- The requirements document says

> 4.3 Replay of BGP UPDATE messages need not be completely prevented, but a BGPsec design MUST provide a mechanism to control the window of exposure to replay attacks.

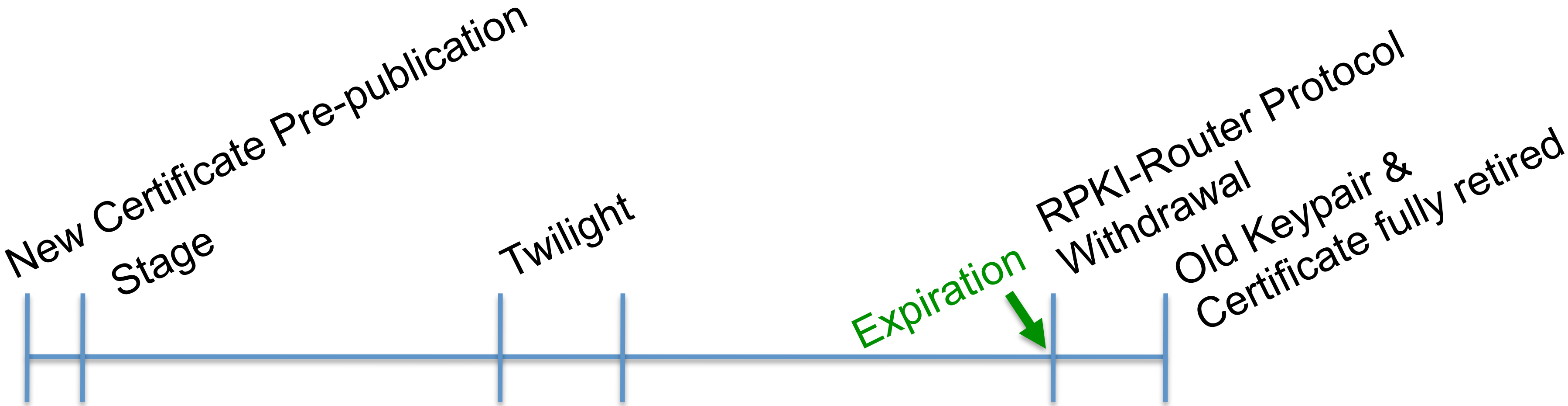
- The "window of exposure" is only open if something about the Update has changed (e.g., AS_PATH first hop)
  - Under normal circumstances, this is infrequent
  - When there is a change, a BGPSEC rollover is about 2 * Cache Update Period +1 * BGP Update Period.
  - Conservative setting of the Expire Time (currently specified in the BGPSEC protocol) may not react in a shorter period
- Note that the use of the Expire Time requires new Updates regardless of whether there is an open window

Conclusions

- It is both necessary and valuable to describe a careful process for BGPSEC router keypair/certificate rollover
- This process can also be used to ensure freshness in the routing system, without changing BGP semantics
- We believe this topic is suitable as a WG deliverable, and would like feedback regarding making this a WG document

Backup Slides

Rollover Timeline
(Certificate Expiration)



New Certificate Pre-publication Stage

Twilight

Expiration

RPKI-Router Protocol Withdrawal

Old Keypair & Certificate fully retired

Generation Timeframe

Cache Update Timeframe

BGP Update Propagation Timeframe

BGP Update Propagation Timeframe

Rollover AS Creates new keypair/ Cert

Rollover AS distributes new Certificate to RPKI Caches

Rollover AS Distributes New Signed Updates

RPKI Caches remove old public key mapping from routers. Routers withdraw routes using old public key

Maintaining the replay window in the RPKI

- It is still possible to maintain a replay window in the RPKI by
  - Choosing a short certificate validation period
  - When there is no need to withdraw a router, re-issue the router certificate with the same public key, but change the key when necessary
- This can be thought of as “beaconing” within the RPKI, but without changing BGP state