BGPSEC Router Certificate Rollover

draft-ietf-sidr-bgpsec-rollover-03

Brian Weis

Roque Gagliano

Keyur Patel

BGPsec Router Keying

- A BGPsec router needs an ECDSA keypair, and an X.509 BGPsec router certificate to disseminate its public key
  - See draft-ietf-sidr-bgpsec-algs-09 & draft-ietf-sidr-rtr-keying-08
- In other applications a device certificate is distributed directly between peers as part of a key agreement protocol, but BGPsec router certificates will be distributed asynchronously through the RPKI
  - Careful synchronization is needed between use of a ECDSA private key and the BGPsec router certificate distribution
  - Of special concern is synchronization when an BGPsec router certificate has been revoked, as there is an urgency to begin using the new keypair
- This draft proposes a method for synchronization, with and without revocation

BGPsec Key Rollover Events (1)

- Routine rollovers
  - BGPSEC scheduled rollover. Expiration date (NotValidAfter) requires a replacement certificate.
  - BGPSEC certificate fields changes. Something in the certificate (such as the AS Resource Identifier or Subject) changes.
- In a routine rollover the public key in the new certificate may not change, in which case BGPsec routers do not need to be aware of the rollover.
- When the keypair does change, the synchronization needs to be orderly but can follow the same timescale as the distribution of RPKI certificates and ROAs.

BGPsec Key Rollover Events (2)

- Urgent rollovers
  - BGPSEC emergency rollover. A compromised key may require the replacement of a BGPSEC certificate.
  - BGPSEC signature anti-replay protection. 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)
- Urgent rollovers require a keypair change to be effective, and the timescale is sensitive to distribution delays.

Steps in the Rollover

- New Certificate Pre-publication
  - Rollover AS generates a new keypair (if needed) and obtains a new certificate for the router(s)
  - If generated elsewhere, keypairs are positioned onto the router(s)
- Staging Period
  - Rollover AS makes the new certificate available to the RPKI global repository and it is propagated and verified by RPKI Caches
  - When a new keypair was distributed the global RPKI-Cache will add the new key to the routers that it manages
- Twilight
  - Rollover AS 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)
- CRL Publication (optional)
  - 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

Keypair Expiration Rollover Timeline

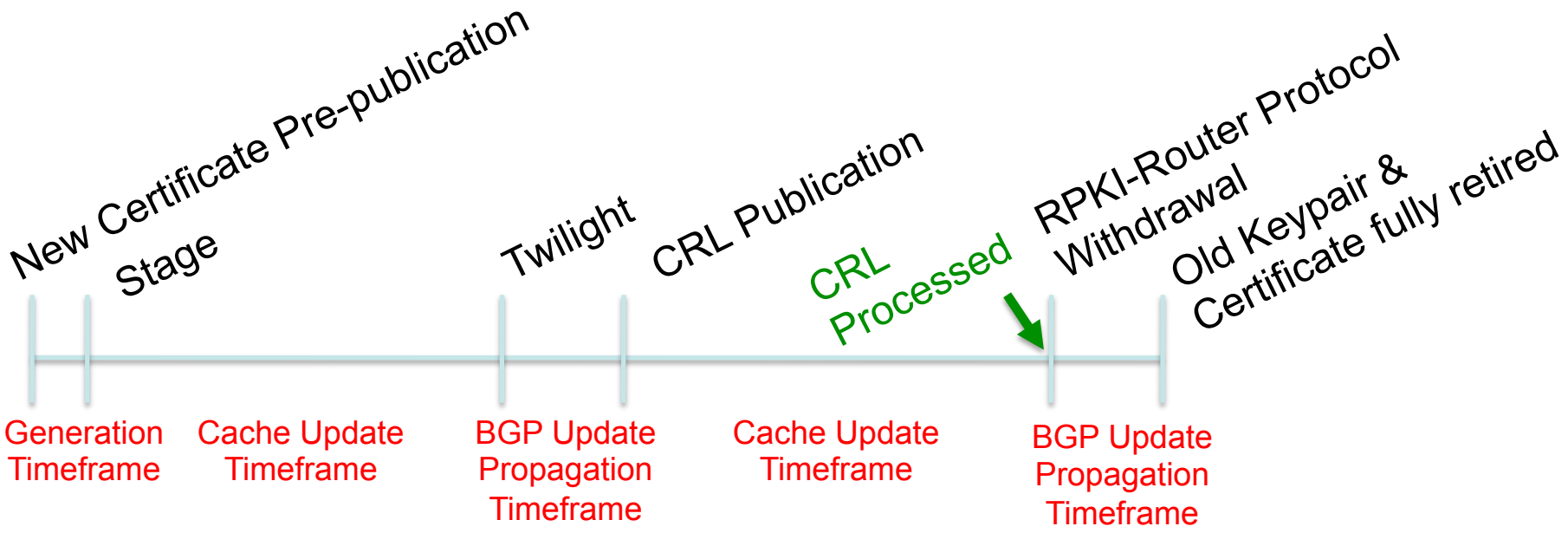
Rollover AS Creates new keypair/ Cert

Rollover AS distributes new Certificate to RPKI Caches

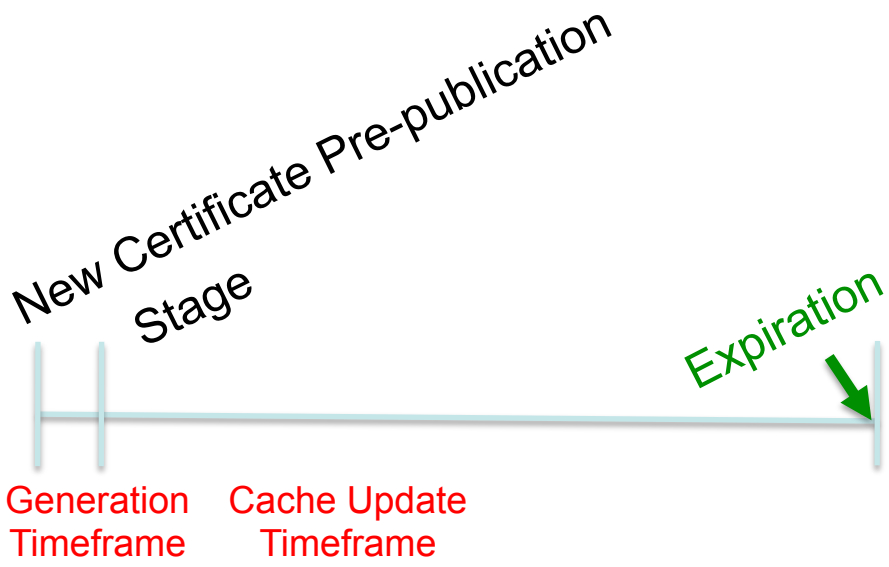
Rollover AS Distributes New Signed BGPsec_Path attributes

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

CRL Rollover Timeline



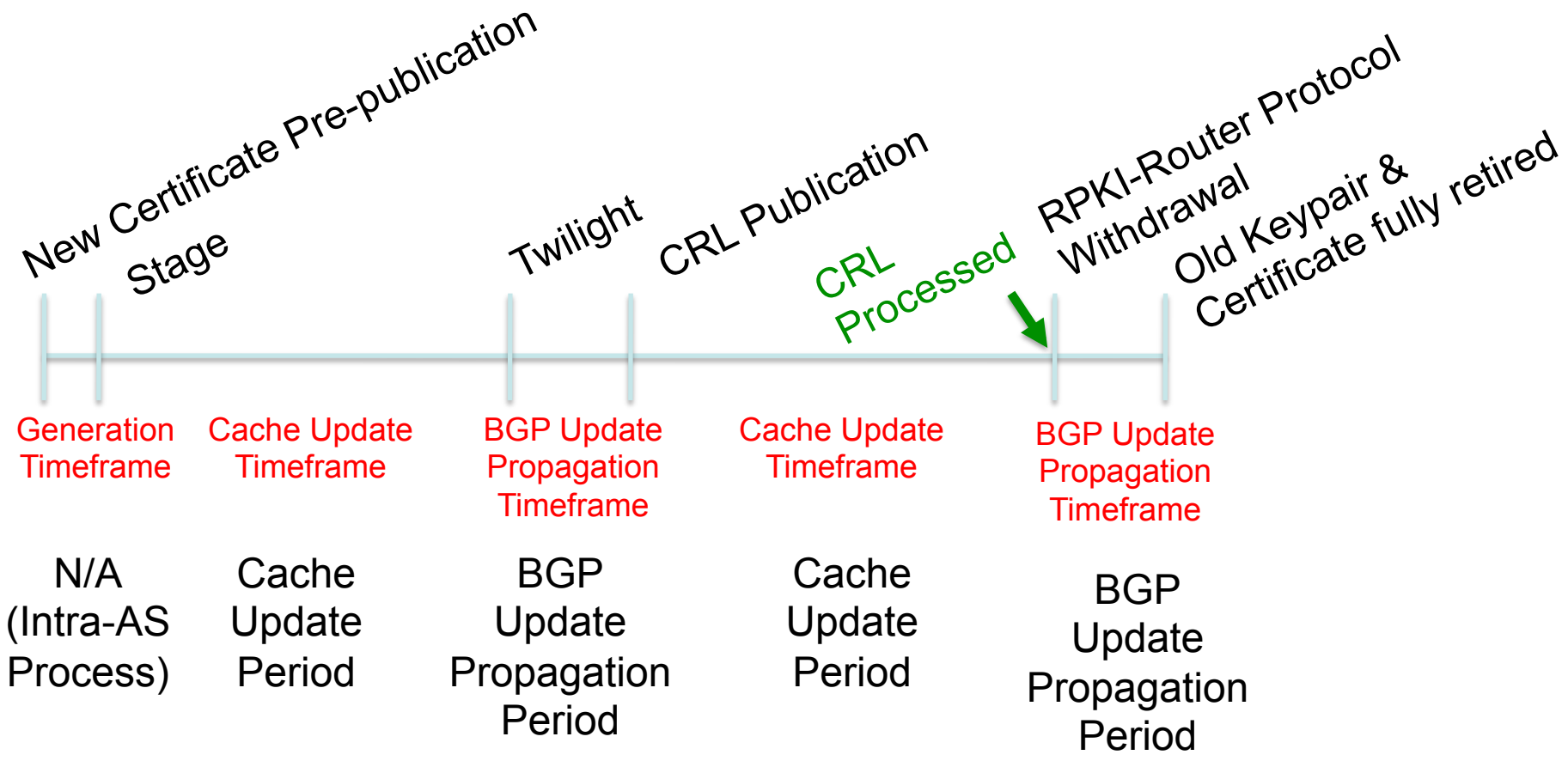
Same Keypair Rollover Timeline



Rollover AS Creates new keypair/ Cert

Rollover AS distributes new Certificate to RPKI Caches

Duration of Timeframes



Timeframe Operational Guidelines

- We don’t yet have operational guidance for the duration of these periods
  - Cache Update Period
  - BGP Update Propagation Periods
- Are there any measurements from current RPKI deployments available?

Origin vs. Transit Signing

- A transit AS that also originates routes in BGP would benefit from distributing two certificates (containing different public keys)
  - One for Origin signatures and one for Transit signatures
  - This protects against having to withdraw Transit signed BGPsec_Path attributes when an Origin keypair/certificate needs to be replaced in an Urgent Rollover
  - This may also enable a longer certificate validity period for Transit signed BGPsec_Path attributes.

Comments & Questions?