

Requirements for Monitoring RPKI-Related Processes on Routers Using BMP

draft-wang-grow-bmp-rpki-mon-reqs-02

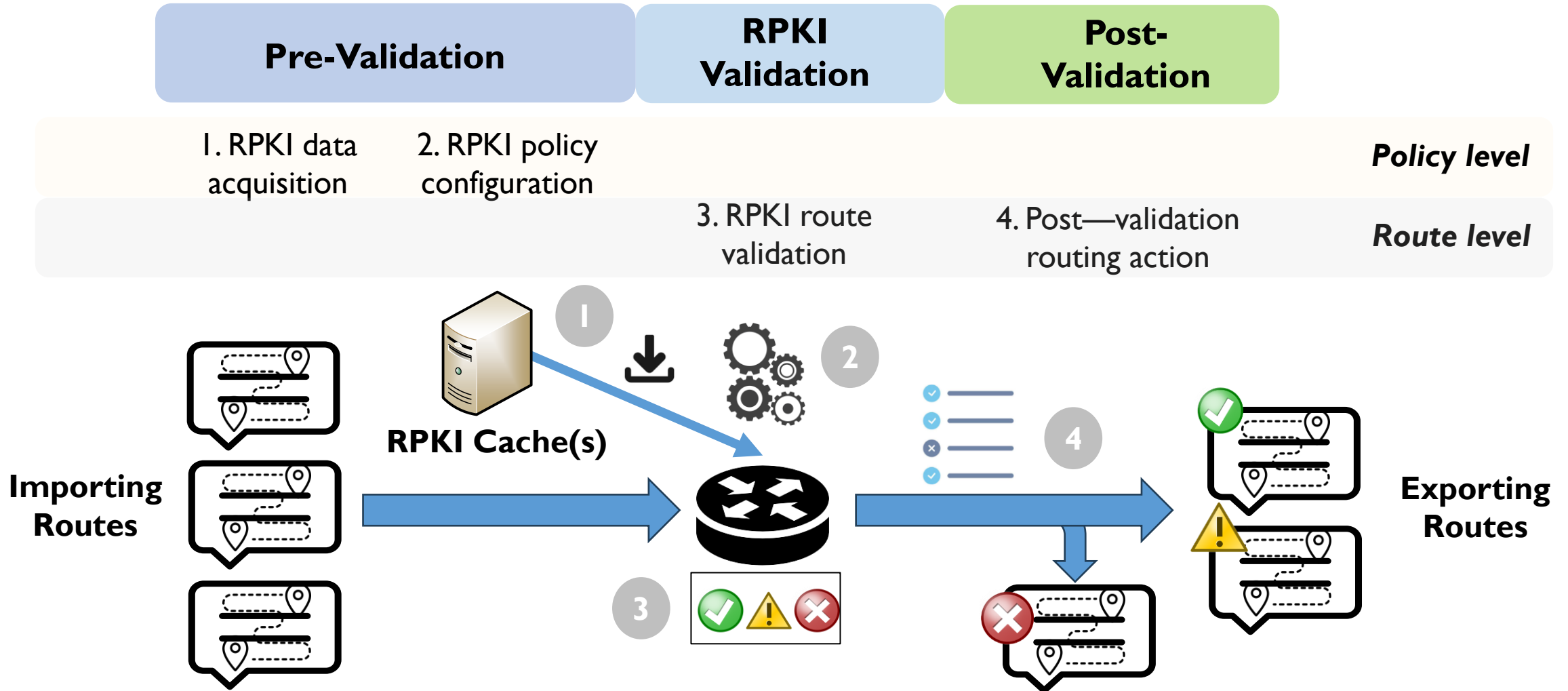
Beijing Zhongguancun Lab, Tsinghua University

Shuhe Wang, Mingwei Xu, Yangyang Wang, Jia Zhang

2026.3

Recap: Requirements Overview

Division of RPKI monitoring stages with BMP:



Key changes in 02

Stage 1: "Data Retrieval from Caches" → "Data Acquisition"

- Extended from RTR-only to multiple RPKI data sources (RTR, iBGP, eBGP, static configuration)

Stage 2: Introduced "route features" to describe large-scale

validation rule sets without transmitting the full set

Stage 3: Enhanced validation structure

- Overall validation state + per-rule validation state
- Support for multiple validation types (origin, path, region validation)

Stage 4: Dedicated RPKI_IMPACT message

(previously relied on bmp-rel Route Event Message)

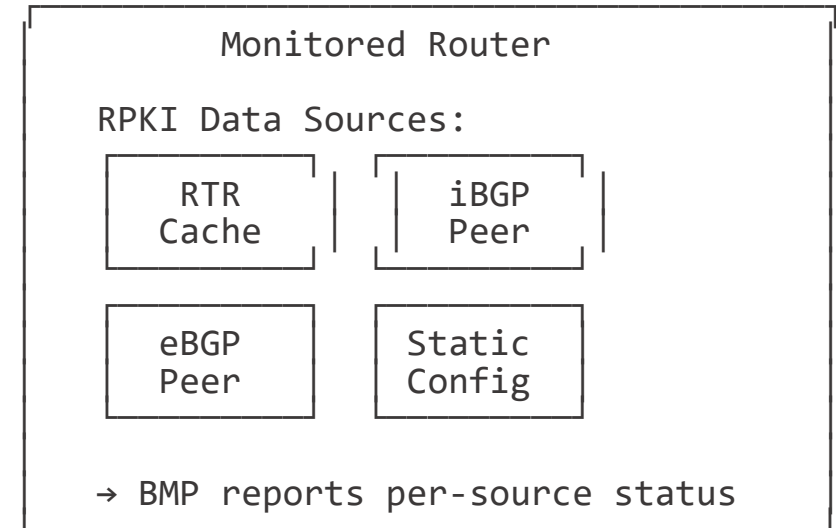
Real router investigation:

- **Capability of RPKI**
 - origin validation
 - path validation
 - region validation
- **Configuration mode**
 - RPKI cache server
 - Static configuration
- **RPKI related policy**
 - prefix origin/aspa-validation enable
 - best-route origin/aspa/region-validation
 - If-match origin/aspa-validation
 - peer advertise origin/aspa-validation

RPKI Data Acquisition: Beyond RTR

Stage I: RPKI data acquisition

- Multiple possible sources
 - RTR connections
 - iBGP connections
 - eBGP connections
 - Static configuration
- **In practice, routers acquire RPKI data from diverse sources**
 - Not limited to RTR (RFC 8210)
 - iBGP/eBGP peers may redistribute RPKI-derived data
 - Static configuration for local overrides
- Common parameters across sources:
 - connection status, data count, sync state, errors
- Source-specific parameters reported via grouped TLVs





Scalable Policy Reporting & Structured Validation

Stage 2 - Policy Configuration

- * Challenge: full validation rule set (all VRPs/ASPAs) can be huge
- * Solution: report "route features" of enabled rules
 - Logical combination (AND/OR) of conditions:
 - ✓ Origin AS within a certain set
 - ✓ Origin AS has a certain role (e.g., customer)
 - ✓ Rule source is static or iBGP only
 - ✓ ...
 - Administrators combine features + per-route info to reconstruct applicable rules

Stage 3 - Route Validation

- * Structured validation report per route:
 - Overall state: Valid / Invalid / Unknown
 - Per validation type applied (origin, path, region...)
 - Per rule: content, source, expiry, specific state
- * Consistency constraint:
 - Valid → all matched rules valid
 - Invalid → at least one matched rule invalid
 - Unknown → no matched rule

Addressing Comments

Comment 1: "RTR protocol state in BMP → scope creep. YANG modeling / streaming telemetry already covers RTR."
Suggestion: "Exclude RPKI-RTR protocol details."

Our response:

- ✓ We agree BMP should not replicate RTR protocol monitoring
- ✓ Draft-02 already shifted from "monitor RTR connections" to "monitor RPKI data sources" — a more abstract framing
- ✓ Our focus: the *effect* of RPKI data on routing decisions, not the operational details of RTR protocol itself
- ✓ BMP and YANG/telemetry are complementary:
 - YANG: RTR session management, protocol operations
 - BMP: RPKI's impact on BGP route validation & selection

Ongoing discussion:

considering CCR hash (draft-ietf-sidrps-rpki-ccr) as a compact database version identifier for Stage I.

Comment 2: "Consider monitoring SLURM (RFC 8416) — local overrides of RPKI validation rules"

Our response:

- ✓ Partially covered by "static configuration" source in Stage I
- ✓ SLURM-specific monitoring (tracking which rules are locally overridden) is a valuable addition → planned for next revision

Simplifying BMP Message Design

Current draft(-02) proposes 5 new message types

```
TBD1: RPKI_SOURCE           (Stage 1)
TBD2: RPKI_POLICY           (Stage 2)
TBD3: RPKI_STAT             (Stage 3 - statistics)
TBD4: RPKI_VALIDATION       (Stage 3 - per-route)
TBD5: RPKI_IMPACT           (Stage 4)
```

Proposed simplification for next revision

```
NEW 1: RPKI_CONFIG
      = merge RPKI_SOURCE + RPKI_POLICY
      Both describe "how RPKI is set up on this router"
      Distinguished by Group TLV sub-types

REMOVED: RPKI_STAT
      → Use existing Stats Report Message
         with new RPKI-specific Stat Type codes
         (aligned with draft-ietf-grow-bmp-bgp-rib-stats)

KEPT: RPKI_VALIDATION (comprehensive, per-route)
KEPT: RPKI_IMPACT     (event-driven, per-route)
```

Benefits

- * Fewer new message types → smaller BMP namespace footprint
- * Better alignment with existing BMP extension ecosystem
- * Source and policy info naturally co-located for correlation
- * Seeking WG feedback on this direction



Discussion Points & Next Steps

1. Message type consolidation:

Is merging RPKI_SOURCE + RPKI_POLICY into RPKI_CONFIG the right direction? Any other simplification ideas?

2. Scope boundary:

Do we have the right balance between RPKI monitoring in BMP vs. YANG/telemetry for RTR protocol state?

3. SLURM (RFC 8416) coverage:

Should local override monitoring be a MUST or SHOULD?

4. Validation type extensibility:

How to best accommodate future validation types (e.g., BGPsec) without protocol revision?

Next steps:

- * Incorporate feedback into future version
- * Multi-vendor router investigation
- * Prototype implementation
- * Integrate with emerging RPKI mechanisms (e.g., CCR hash for database versioning)