Requirements for Monitoring RPKI-Related Processes on Routers Using BMP

draft-wang-grow-bmp-rpki-mon-reqs-01

Beijing Zhongguancun Lab, Tsinghua University

Shuhe Wang, Mingwei Xu, Yangyang Wang, Jia Zhang

2025.07

Difference with last talk

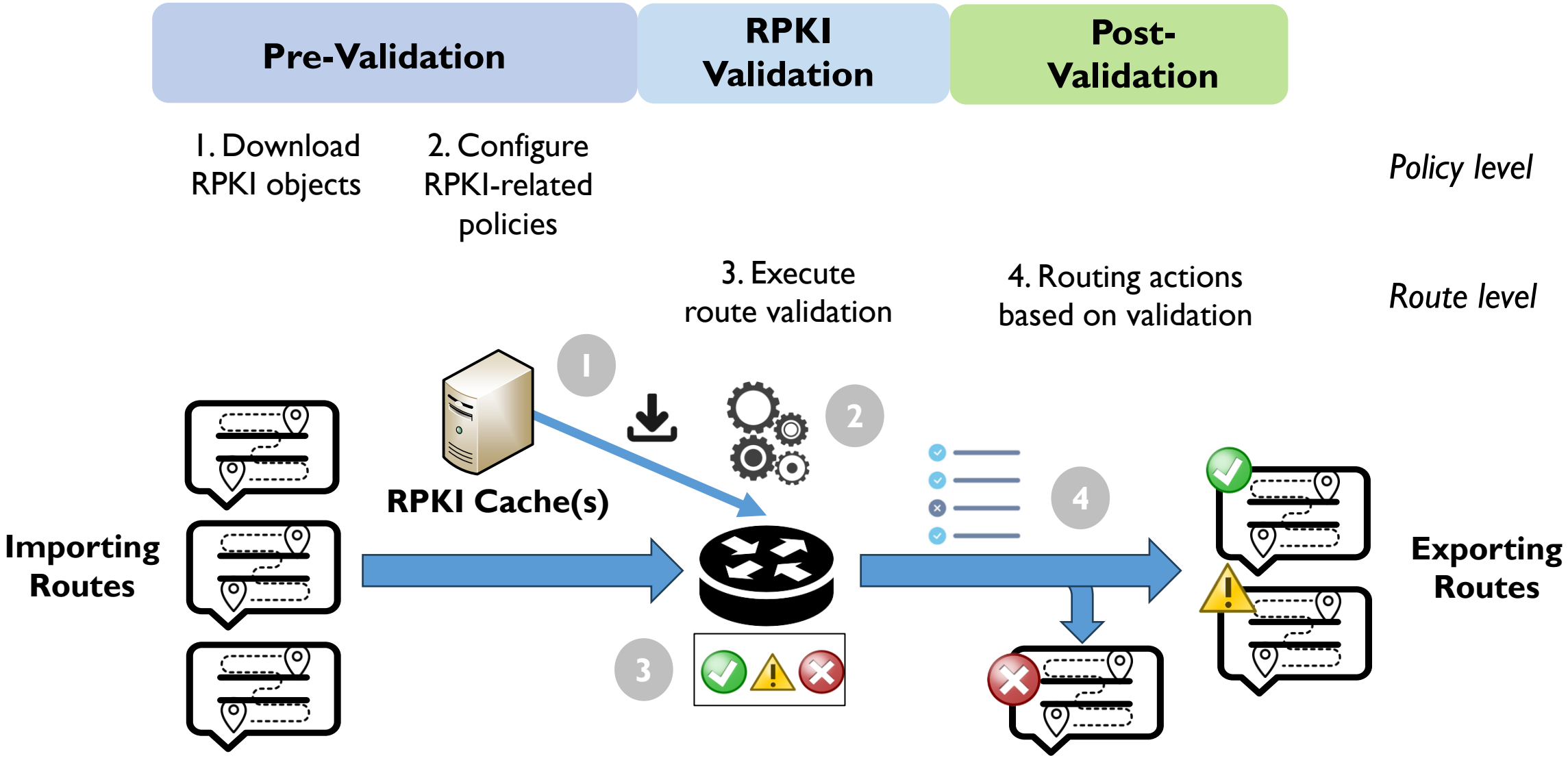
Last talk in IETF 122

- Mainly introduce what kinds of RPKI-related information could be monitored on the router, and why they are important to monitor

Current talk in IETF 123

- Further detail the systematic requirements on monitoring RPKI with BMP
- Give suggestions on extending the current BMP messages
- Emphasize the related security concerns

RPKI-Related Processes on Routers

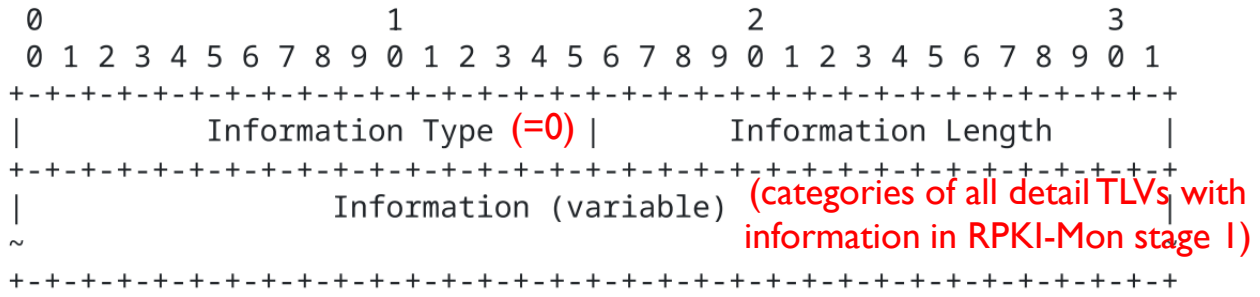


Requirements for Supporting RPKI in BMP

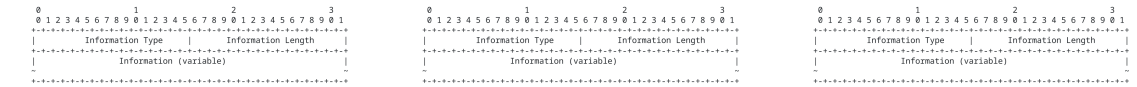
RPKI-Mon stage 1: RPKI data retrieval

- **Monitored fields**
  - RTR connection parameters
    - E.g.: RTR protocol version, connection type, IP address and Port of RPKI cache, etc.
  - Synchronization details
    - E.g.: total number of RPKI records, synchronization state, timestamp of the last successful synchronization, etc.
  - Error metrics
    - E.g.: counts of timeouts, failed synchronization attempts, etc.
- **Suggested message form**
  - Extend the Initiation Message
    - Use a group of information TLVs

Main TLV



Detail TLVs

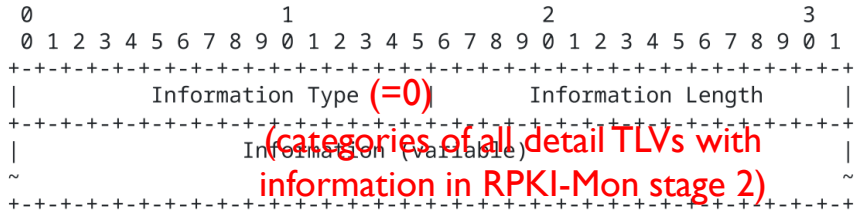


Requirements for Supporting RPKI in BMP

RPKI-Mon stage 2: RPKI-related policy configuration

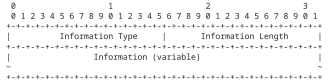
- **Monitored fields**
  - Enablement of RPKI validation
    - Whether the peer is enabled with ROV/ASPA/other RPKI-related validations
  - RPKI-related validation rules
    - set of VRPs/ASPA entries to use for each single peer
  - RPKI-related policies in pre-validation phase (validation results are different w/o the policies)
    - E.g.: route aggregation / route de-aggregation
  - RPKI-related policies in post-validation phase
    - E.g.: filtering / priority reduction / tagging of invalid / unknown routes
- **Suggested message form**
  - Extend the Peer Up Notification Message
    - Use a group of information TLVs

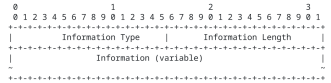
Main TLV



(categories of all detail TLVs with information in RPKI-Mon stage 2)

Detail TLVs

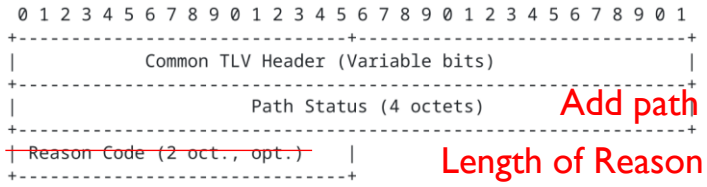




Requirements for Supporting RPKI in BMP

RPKI-Mon stage 3: RPKI-related route validation

- **Monitored fields**
  - Statistical summaries of validation outcomes, aggregated per peer
    - E.g.: Counts of routes in each state, number of filtered routes because of RPKI validation, etc.
  - The validation state of each route, along with the specific reason for that state
    - The relevant VRP/ASPA entry that leads to the validation result, e.g.: prefix length exceeding maxLength, origin AS mismatched, AS path violating ASPA, etc.
- **Suggested message forms**
  - Extend the Statistics Report Message for statistical summaries
    - Extend BMP Statistics Types
    - Existing draft: draft-ietf-grow-bmp-bgp-rib-stats
  - Extend the Route Monitoring Message (of rib-in or loc-rib) for route validation results
    - Extend the Path Status TLV
    - Existing draft: draft-ietf-grow-bmp-path-marking-tlv



Add path status codes for all validation states (valid, invalid, unknown)

Replace Reason Code with Reason String

Length of Reason String should be variable (for relevant VRP and ASPA entry)

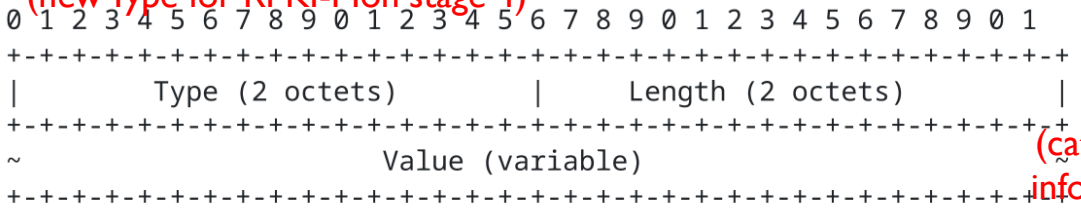
Requirements for Supporting RPKI in BMP

RPKI-Mon stage 4: RPKI-related impact on routing decisions

- **Monitored fields:**
  - For routes influenced by RPKI validation (dropped or priority get changed):
    - Competing routes (if any)
    - Triggered RPKI-related pre-validation policies (if any)
    - Triggered RPKI-related post-validation policies (if any)
- **Suggested message forms**
  - Extend the Route Monitoring Message (of loc-rib or rib-out) for route validation results
    - Extend the TLV in route monitoring

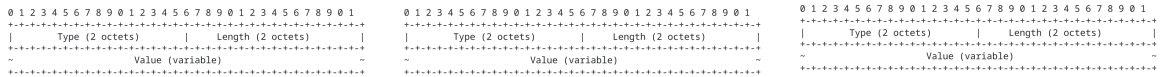
(new Type for RPKI-Mon stage 4)

Main TLV



(categories of all detail TLVs with information in RPKI-Mon stage 4)

Detail TLVs



Other concerns

Security Concerns

- Transmission security
  - Safe transmission protocol (TLS, TCP-AO, etc)
  - End-to-end data validation

- Operational security
  - RTR Protocol transparency
  - Forward compatibility

Thank you!

Suggestions and comments are welcome!