SIDR Operations Working Group
Internet-Draft
Intended status: Standards Track
Expires: 2 September 2026

Y. Fu
Zhongguancun Laboratory
M. Xu
Tsinghua
Y. Wang
Tsinghua University
J. Zhang
Y. Zhang
Zhongguancun Laboratory

1 March 2026

Operational Monitoring of RPKI Repositories Health and Safety
draft-fu-sidrops-rpki-repositories-monitoring-00

Abstract

The Resource Public Key Infrastructure (RPKI) relies on a globally distributed set of repositories to deliver signed routing authorization data to Relying Parties (RPs). Internet Service Providers (ISPs) depend on RPs to collect RPKI objects from distributed repositories and validate them cryptographically, resulting in hundreds of thousands of Validated Route origin authorization Payloads (VRPs). Nevertheless, even with multiple RPs deployed, ISPs have limited insight into the operational health and reliability of each repository. When a large number of ROAs suddenly change from valid to unknown or invalid, operators often lack sufficient information to diagnose the cause, which may stem from an outage or instability in a specific repository. Consequently, ISPs cannot easily determine whether these changes are caused by routine updates, malicious behavior, or underlying repository instability.

Consequently, ISPs cannot easily determine whether these changes are caused by routine updates, malicious behavior, or underlying repository instability. This document provides operational guidance for monitoring the health and safety of RPKI repositories on a per-repository basis. It defines measurable indicators related to reachability, availability, and content integrity, and explains how these metrics can be used to detect degraded performance or potentially unsafe repository behavior. The document discusses and provides recommendations for repositories alerting and operational response. The goal is to improve the transparency, operational availability and security of the RPKI ecosystem.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

This Internet-Draft will expire on 2 September 2026.

Copyright Notice

Table of Contents

1. Introduction 3
  1.1. Requirements Language 4
2. Problem Statement 4
3. Metric Model 5
  3.1. Overview 5
  3.2. Observation Window 5
4. Base Counters 5
  4.1. Transport Counters 5
  4.2. Synchronization Counters 6
  4.3. Object Retrieval Counters 6
  4.4. Validation Counters 6
  4.5. Repository Update Time 6
5. Derived Health Indicators 6
  5.1. Reachability Indicators 6
    5.1.1. Transport Reachability Ratio (TRR) 6
    5.1.2. DNS Resolution Success Rate (DRSR) 7
  5.2. Availability Indicators 7
    5.2.1. Fetch Success Ratio (FSR) 7
    5.2.2. Synchronization Success Ratio (SSR) 7
    5.2.3. Update Freshness (UF) 7

5.3. Content Integrity Indicators 7
5.3.1. Validation Success Ratio (VSR) 7
5.3.2. Object Consistency Ratio (OCR) 7
5.3.3. Hash Mismatch Rate (HMR) 8
5.4. Alerting Guidance 8
6. State-Change and Churn Indicators 8
6.1. Overview 8
6.2. Snapshot Model 8
6.3. General Object Churn 8
6.3.1. Object Change Count (OCC) 9
6.3.2. Object Change Ratio (OCRate) 9
6.4. ROA Stability Indicators 9
6.4.1. ROA Count Delta (RCD) 9
6.4.2. ROA Change Ratio (RCR) 9
6.4.3. ROA Withdrawal Ratio (RWR) 10
6.5. Certificate and CA Stability Indicators 10
6.5.1. Certificate Change Ratio (CCR) 10
6.5.2. Expired Object Ratio (EOR) 10
6.5.3. Invalid Object Ratio (IOR) 10
6.6. RRDP Publication Continuity 10
6.6.1. Serial Progression Delta (SPD) 10
6.6.2. Delta Volume (DV) 10
6.7. Alerting Guidance 11
7. Security Considerations 11
8. IANA Considerations 11
9. References 11
9.1. Normative References 11
9.2. Informative References 11
Authors' Addresses 12

1. Introduction

The Resource Public Key Infrastructure (RPKI) architecture is described in [RFC6480]. It defines a framework that represents the allocation hierarchy of IP address space and Autonomous System (AS) numbers, as well as a distributed repository system for the storage and dissemination of the signed objects used to improve routing security. Internet Service Providers (ISPs) and other participants rely on Relying Parties (RPs) to retrieve and validate this published information from the repositories. RP uses rsync protocol and RPKI Repository Delta Protocol (RRDP) protocol for efficient synchronization of repository contents. The rsync protocol and RPKI Repository Delta Protocol (RRDP) are described in [RFC5718] and [RFC8182]. An operational best current practices for deployment and management of an RPKI Publication Server is described in [I-D.ietf-sidrops-publication-server-bcp-profile].

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Problem Statement

The RPKI infrastructure consists of a large and growing number of independently operated repositories distributed across multiple networks, organizations, and geographic regions. Internet Service Providers (ISPs) depend on Relying Parties (RPs) to collect RPKI objects from the distributed repositories and validate them cryptographically, resulting in hundreds of thousands of Validated ROA Payloads (VRPs).

However, even with multiple RPs deployed, ISPs have limited insight into the operational health and reliability of each repository. Because RPs generally treat all repositories uniformly and do not maintain a persistent behavioral profile for each repository. When a large number of ROAs suddenly change from valid to unknown or invalid, operators often lack sufficient information to diagnose the cause, which may stem from an outage or instability in a specific repository. Meanwhile, not all repositories are well maintained— some are unreachable, and others contain outdated objects. As a result, ISPs lack clear visibility into the status of each repository.

At present, ISPs lack the ability to distinguish whether changes in RPKI objects are due to routine updates, malicious behavior, or systemic issues within the repositories. In the absence of consistent per-repository monitoring and operational visibility, operators face significant challenges in identifying degraded repositories, correlating incidents across networks, and proactively detecting emerging risks.

This document seeks to address these gaps. It provides operational guidance for monitoring the health and safety of RPKI repositories on a per-repository basis. It identifies measurable indicators related to reachability, availability, content integrity. It describes how these indicators can be used to detect degraded or unsafe repository behavior. The document discusses and provides recommendations for repositories alerting and operational response. The goal is to improve the transparency, operational availability and security of the RPKI ecosystem.

3. Metric Model

3.1. Overview

This section summarizes all metrics defined in this document.

Metrics are divided into three classes:

Base Counters: Primitive observable events. Used for diagnostics and as inputs to derived metrics.

Health Indicators:Ratios or computed values representing instantaneous repository correctness and usability. These indicators SHOULD be used for alerting.

State-Change (Churn) Indicators: Metrics representing differences between successive repository snapshots. These indicators detect abnormal or unexpected publication behavior over time.

Monitoring systems:

MUST implement Base Counters,

MUST compute Health Indicators,

SHOULD compute State-Change Indicators.

3.2. Observation Window

Indicators SHOULD be computed over a configurable time window. Windows MAY be sliding or tumbling. Implementations SHOULD document the window duration.

4. Base Counters

Counters defined in this section are per repository and per transport unless otherwise stated.

4.1. Transport Counters

attempted_connections: Number of connection attempts initiated.

successful_connections: Number of successful connections.

failed_connections: Number of unsuccessful connections.

successful_dns_resolutions: Number of successful DNS queries.

total_dns_queries: Number of total DNS queries.

4.2. Synchronization Counters

attempted_syncs: Number of synchronization attempts.

successful_syncs: Number of synchronization attempts completed without error.

failed_syncs: Number of synchronization attempts that failed.

4.3. Object Retrieval Counters

attempted_object_fetches: Number of objects such as ROA, Certificates,manifest, CRL etc.

successful_object_fetches: Number of objects download successful.

failed_object_fetches: Number of objects downloaded failed.

4.4. Validation Counters

total_objects: Number of total objects, such as ROA, certificates.

valid_objects: Number of valid objects.

invalid_objects: Number of invalid objects.

referenced_objects: Number of objects in manifest file.

present_referenced_objects: The actual downloaded objects.

4.5. Repository Update Time

observed_repository_update: Observed repository update time.

5. Derived Health Indicators

The indicators defined in this section measure the instantaneous operational health of a repository, including reachability, availability, and integrity.

5.1. Reachability Indicators

5.1.1. Transport Reachability Ratio (TRR)

TRR = successful_connections / attempted_connections

Measures probability that the repository endpoint can be contacted.

5.1.2. DNS Resolution Success Rate (DRSR)

DRSR = successful_dns_resolutions / total_dns_queries

Detects DNS-related failures.

5.2. Availability Indicators

5.2.1. Fetch Success Ratio (FSR)

FSR = successful_object_fetches / attempted_object_fetches

Measures reliability of object delivery.

5.2.2. Synchronization Success Ratio (SSR)

SSR = successful_syncs / attempted_syncs

Measures probability that a complete update can be obtained.

Persistent low values indicate degraded availability.

5.2.3. Update Freshness (UF)

UF = now − last_observed_repository_update

UF measures repository staleness and is time-based rather than a ratio.

5.3. Content Integrity Indicators

5.3.1. Validation Success Ratio (VSR)

VSR = valid_objects / total_objects

Indicates cryptographic and syntactic validity.

5.3.2. Object Consistency Ratio (OCR)

OCR = present_referenced_objects / referenced_objects

referenced_objects= files the manifest says must exist

present_referenced_objects= files actually download successfully

5.3.3. Hash Mismatch Rate (HMR)

HMR = hash_mismatches / hash_verifications

Non-zero values MUST be treated as critical integrity failures.

5.4. Alerting Guidance

Monitoring systems SHOULD generate alerts when TRR, SRR, FSR,OCR, HMR falls below a configured threshold value.

6. State-Change and Churn Indicators

6.1. Overview

A repository MAY remain fully reachable and internally consistent while exhibiting abnormal or unsafe publication behavior. Examples include: sudden bulk withdrawal of ROAs, excessive object churn, incomplete or partially applied updates. Such events can materially affect routing outcomes even when health indicators remain nominal.

To detect these conditions, monitoring systems should evaluate state-change indicators—also known as churn indicators—that measure the differences between consecutive repository states. When the change in these indicators exceeds an ISP-configured threshold, the monitoring system sends an alarm.

These indicators provide temporal visibility and enable detection of unexpected or anomalous repository behavior.

6.2. Snapshot Model

After each successful synchronization, a monitoring system SHOULD construct a repository snapshot containing at least:

validated object identifiers,

object hashes,

object types (ROA, certificate, CRL, manifest, etc.),

RRDP session identifiers and serial numbers.

Change indicators are computed by comparing the current snapshot with the most recent prior successful snapshot.

6.3. General Object Churn

6.3.1. Object Change Count (OCC)

OCC = added_objects + removed_objects + modified_objects

added_objects are objects newly observed,

removed_objects are previously observed objects no longer present,

modified_objects are objects whose content hash has changed.

OCC provides an absolute measure of repository churn.

6.3.2. Object Change Ratio (OCRate)

OCRate = OCC / previous_total_objects

This indicator normalizes churn by repository size and enables comparison across repositories.

Large values MAY indicate: bulk re-publication, tooling errors, storage faults, or abnormal behavior.

Monitoring systems SHOULD track historical baselines for this value.

6.4. ROA Stability Indicators

Because ROAs directly affect route validation outcomes, their stability is particularly important.

6.4.1. ROA Count Delta (RCD)

RCD = added_roas + removed_roas + modified_roas

Large negative values MAY indicate accidental withdrawal

Large positive values MAY indicate bulk reissuance.

6.4.2. ROA Change Ratio (RCR)

RCR = (added_roas + removed_roas + modified_roas) / previous_roa_count

Measures relative ROA churn.

Persistent or sudden spikes SHOULD generate alerts.

6.4.3. ROA Withdrawal Ratio (RWR)

RWR = removed_roas / previous_roa_count

Unexpectedly large withdrawal ratios exceeds the configured threshold by ISP SHOULD send an alarm.

6.5. Certificate and CA Stability Indicators

6.5.1. Certificate Change Ratio (CCR)

CCR = (added_certs + removed_certs + modified_certs) / previous_cert_count

Large values MAY indicate:key rollover, mass reissuance, misconfiguration, or abnormal behavior.

6.5.2. Expired Object Ratio (EOR)

EOR = expired_objects / total_objects

Expired objects SHOULD NOT normally appear in a properly maintained repository.

Values greater than zero SHOULD trigger alerts.

6.5.3. Invalid Object Ratio (IOR)

IOR = invalid_objects / total_objects

Increasing IOR over time MAY indicate publication or signing defects.

6.6. RRDP Publication Continuity

6.6.1. Serial Progression Delta (SPD)

SPD = current_serial − previous_serial

The SPD 0.

6.6.2. Delta Volume (DV)

DV = number_of_objects_changed_in_rrdp_delta

Large deltas MAY indicate excessive churn.

6.7. Alerting Guidance

Monitoring systems SHOULD generate alarms when: RCR or CCR significantly exceed historical norms, RWR, EOR exceeds an operator-defined threshold, SPD 0 unexpectedly.

7. Security Considerations

This document defines operational monitoring metrics for assessing the reachability, availability, integrity, and stability of RPKI repositories. It does not modify the RPKI trust model, cryptographic validation procedures, or protocol behavior.

8. IANA Considerations

This document has no IANA actions

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC6480] Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", RFC 6480, DOI 10.17487/RFC6480, February 2012, <https://www.rfc-editor.org/info/rfc6480>.

[RFC5718] Beller, D. and A. Farrel, "An In-Band Data Communication Network For the MPLS Transport Profile", RFC 5718, DOI 10.17487/RFC5718, January 2010, <https://www.rfc-editor.org/info/rfc5718>.

[RFC8182] Bruijnzeels, T., Muravskiy, O., Weber, B., and R. Austein, "The RPKI Repository Delta Protocol (RRDP)", RFC 8182, DOI 10.17487/RFC8182, July 2017, <https://www.rfc-editor.org/info/rfc8182>.

9.2. Informative References

[I-D.ietf-sidrops-publication-server-bcp-profile]
Bruijnzeels, T., Kock, T., Hill, F., and T. Harrison, "RPKI Publication Server Best Current Practices", Work in Progress, Internet-Draft, draft-ietf-sidrops-publication-servere-bcp, 20 October 2025, <https://datatracker.ietf.org/doc/draft-ietf-sidrops-publication-server-bcp/05/>.

Authors' Addresses

Yonghong Fu
Zhongguancun Laboratory
Beijing
China
Email: fuyh@mail.zgclab.edu.cn

Mingwei Xu
Tsinghua
Beijing
China
Email: xmw@cernet.edu.cn

Yangyang Wang
Tsinghua University
Beijing
China
Email: wyy@cernet.edu.cn

Jia Zhang
Zhongguancun Laboratory
Beijing
China
Email: zhangj@mail.zgclab.edu.cn

Yuanyuan Zhang
Zhongguancun Laboratory
Beijing
China
Email: zhangyy@zgclab.edu.cn