Network Working Group
Internet-Draft
Updates: 6841 (if approved)
Intended status: Standards Track
Expires: May 7, 2020

T. Bruijnzeels
NLnet Labs

November 4, 2019

Resource Public Key Infrastructure (RPKI) Repository Requirements draft-sidrops-bruijnzeels-deprecate-rsync-00

Abstract

This document updates the profile for the structure of the Resource Public Key Infrastructure (RPKI) distributed repository [RFC6481] by describing how the RPKI Repository Delta Protocol (RRDP) [RFC8182] can be used, and stipulating that repositories which are made available over RRDP are no longer required to be available over rsync.

The Profile for X.509 PKIX Resource Certificates [RFC6487] uses rsync URIs in the Authority Information Access, Subject Information Access, and CRL Distribution Points extensions. This document leaves this unchanged, meaning that rsync URIs are still used for naming and finding objects in the RPKI. However, it is no longer guaranteed that objects can be retrieved using these URIs.

Status of This Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on May 7, 2020.

Table of Contents

1. Requirements notation 2
2. Motivation 2
3. Rsync URIs as object identifiers 3
4. Updates to RFC6481 3
5. Deployment Considerations 4
5.1. RRDP support in RPKI Repositories 4
5.2. RRDP support in Relying Party software 5
6. IANA Considerations 5
7. Security Considerations 5
8. Acknowledgements 5
9. Normative References 5
Author's Address 6

1. Requirements notation

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. Motivation

The Resource Public Key Infrastructure (RPKI) [RFC6480] as originally defined uses rsync as its distribution protocol, as outlined in [RFC6481]. Later, the RPKI Repository Delta Protocol (RRDP) [RFC8182] was designed to provide an alternative. In order to facilitate incremental deployment RRDP has been deployed as an additional optional protocol, while rsync was still mandatory to implement.

RPKI Repository operators are still required to provide 24/7 up-time to their rsync infrastructure, as long as the requirement to support rsync stands. Thus, the benefit that they get from supporting RRDP, which enables the use of content delivery networks (CDNs) for this purpose, is limited.

And as long as not all RPKI Repositories support RRDP, Relying Party software is still required to support rsync. Because there is a lack of rsync client libraries, this is typically implemented by calling a system installed rsync binary. This is inefficient, and has issues with regards to versioning of the rsync binary, as well as reporting errors reliably.

This document requires that all RPKI repositories and all Relying Parties support RRDP. It also stipulates that these parties are no longer required to support rsync. This way all parties are freed of direct operational dependencies on rsync.

3. Rsync URIs as object identifiers

[RFC6481] defines a profile for the Resource Certificate Repository Structure. In this profile objects are identified through rsync URIs. E.g. a CA certificate has an Subject Information Access descriptor which uses an rsync URI to identify its manifest [RFC6486]. The manifest enumerates the relative names and hashes, for all objects published under the private key of the CA certificate. This the full rsync URI identifiers for each object can be resolved relative to the manifest URI.

Though it would be possible in principle to build up an RPKI tree hierarchy of objects based on key identifiers and hashes [RFC8488], most Relying Party implementations have found it very useful to use rsync URIs for this purpose. Furthermore, these identifiers make it much easier to name object in case of validation problems, which help operators to address issues.

For these reasons, RRDP still includes rsync URIs in the definition of the publish, update and withdraw elements in the snapshot and delta files that it uses. See section 3.5 of [RFC8182]. Thus, objects retrieved through RRDP can be mapped easily to files and URIs, similar to as though rsync would have been used to retrieve them.

4. Updates to RFC6481

OLD:

- The publication repository SHOULD be hosted on a highly available service and high-capacity publication platform.

- The publication repository MUST be available using rsync [RFC5781] [RSYNC]. Support of additional retrieval mechanisms is the choice of the repository operator. The supported retrieval mechanisms

MUST be consistent with the accessMethod element value(s) specified in the SIA of the associated CA or EE certificate.

NEW:

- The publication repository MUST be available using the RPKI Repository Delta Protocol [RFC8182]. The RRDP server SHOULD be hosted on a highly available platform.

- The publication repository MAY be available using rsync [RFC5781].

- Support of additional retrieval mechanisms is the choice of the repository operator. The supported retrieval mechanisms MUST be consistent with the accessMethod element value(s) specified in the SIA of the associated CA or EE certificate.

5. Deployment Considerations

Relying Parties can drop support for rsync only when all RPKI repositories support RRDP.

RPKI repositories can drop support for rsync only when Relying Parties support RRDP. Even when all actively maintained RP software packages support RRDP, there will still be old versions of the software in operational use. It is most likely impossible to find that all deployed software supports RRDP, but since RRDP SHOULD be used when it is available [section 3.4.1 of @!RFC8182] it will be possible to measure adoption.

5.1. RRDP support in RPKI Repositories

[This section can be updated during discussion of this document, and may be removed before possible publication.]

Repository Implementation	Support for RRDP
afrinic	planned
apnic	yes
arin	under development
lacnic	planned
ripe ncc	yes
rpki.net	yes(1)
krill	yes(2)

(1) in use at various National Internet Registries, as well as other resource holders under RIRs. (2) Software under development.

5.2. RRDP support in Relying Party software

[This section can be updated during discussion of this document, and may be removed before possible publication.]

Relying Party Implementation	Support for RRDP
FORT	no
OctoRPKI	yes
rcynic	yes
RIPE NCC RPKI Validator 2.x	yes
RIPE NCC RPKI Validator 3.x	yes
Routinator	yes
rpki-client	no
RPSTIR	yes

6. IANA Considerations

This document has no IANA actions.

7. Security Considerations

TBD

8. Acknowledgements

TBD

9. 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>.

[RFC5781] Weiler, S., Ward, D., and R. Housley, "The rsync URI Scheme", RFC 5781, DOI 10.17487/RFC5781, February 2010, <https://www.rfc-editor.org/info/rfc5781>.

[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>.

[RFC6481] Huston, G., Loomans, R., and G. Michaelson, "A Profile for Resource Certificate Repository Structure", RFC 6481, DOI 10.17487/RFC6481, February 2012, <https://www.rfc-editor.org/info/rfc6481>.

[RFC6486] Austein, R., Huston, G., Kent, S., and M. Lepinski, "Manifests for the Resource Public Key Infrastructure (RPKI)", RFC 6486, DOI 10.17487/RFC6486, February 2012, <https://www.rfc-editor.org/info/rfc6486>.

[RFC6487] Huston, G., Michaelson, G., and R. Loomans, "A Profile for X.509 PKIX Resource Certificates", RFC 6487, DOI 10.17487/RFC6487, February 2012, <https://www.rfc-editor.org/info/rfc6487>.

[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>.

[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>.

[RFC8488] Muravskiy, O. and T. Bruijnzeels, "RIPE NCC's Implementation of Resource Public Key Infrastructure (RPKI) Certificate Tree Validation", RFC 8488, DOI 10.17487/RFC8488, December 2018, <https://www.rfc-editor.org/info/rfc8488>.

Author's Address

Tim Bruijnzeels
NLnet Labs

Email: tim@nlnetlabs.nl
URI: https://www.nlnetlabs.nl/