

IETF SIDROPS WG Update

Di Ma

Principal Research Fellow at ZDNS

madi@rpstir.net

APNIC 50 Routing Security SIG Meeting

RPKI is ready to support Secure Inter-domain Routing.

- IETF Secure Inter-Domain Routing (SIDR) WG (**Concluded**) has defined the RPKI.
- The RPKI is designed to support the validation of BGP Origin (ROV, RFC 6811) and BGP Path authorization (BGPsec, RFC 8205) and more...
 - IP Address to ASN (Route Origin Authorization, RFC 6482)
 - ASN to Router (Router Certificate, RFC 8209)

RPKI is right in use of supporting Secure Inter-domain Routing.

- All 5 RIRs offer production service today.
 - RPKI adoption is promising both in IPv4 and IPv6 address spaces.
 - More complete support (ISPs acting as CAs) is available from the RIRs.
- RPKI-based ROV is rolling out within increasing numbers of IXP/ISP/ICP worldwide.
- Vendors are supporting ROV.
 - Cisco, Huawei, Juniper...
- RPKI is also recommended by Mutually Agreed Norms for Routing Security (MANRS), initiated by ISOC.



| NAME | TYPE | DETAILS | STATUS | ASN |
|-----------------------|---------|-------------------------------|----------------|-------|
| Telia | transit | signed + filtering | safe | 1299 |
| Cogent | transit | signed + filtering | safe | 174 |
| GTT | transit | signed + filtering | safe | 3257 |
| NTT | transit | signed + filtering | safe | 2914 |
| Hurricane Electric | transit | signed + filtering | safe | 6939 |
| Cloudflare | cloud | signed + filtering | safe | 13335 |
| Wikimedia Foundation | cloud | signed + filtering | safe | 14907 |
| Scaleway | cloud | signed + filtering | safe | 12876 |
| TATA | transit | filtering peers only | partially safe | 6453 |
| PCCW | transit | filtering peers only | partially safe | 3491 |
| Telstra International | transit | signed | partially safe | 4637 |
| AT&T | ISP | signed + filtering peers only | partially safe | 7018 |
| Amazon | cloud | signed | partially safe | 16509 |

isbgpsafeyet.com by Cloudflare

| date | RIR | IPv4 adoption | IPv6 adoption |
|----------|---------|---------------|---------------|
| 20200731 | afrinic | 0.1014 | 0.0503 |
| 20200731 | arin | 0.1144 | 0.0365 |
| 20200731 | lacnic | 0.2590 | 0.3464 |
| 20200731 | apnic | 0.1609 | 0.1424 |
| 20200731 | ripencc | 0.4425 | 0.2818 |

RPKI Adoption Statistics by NRO

Operation is yet another important thing.

- A set of technical standards could be a mighty guide but not a prerequisite for success of the RPKI operation in practice.
- RPKI-based routing validation in a larger scale calls for best practice.
- The SIDR Operations Working Group (SIDROPS) Charter
 - To develop guidelines for the operation of SIDR-aware networks
 - To provide operational guidance on how to deploy and operate SIDR technologies in existing and new networks

Years of RPKI-based routing security practice calls for retrofits by IETF.

- Standards
 - Manifest Update, [draft-ietf-sidrops-6486bis-00](#)
 - Path Validation by ASPA (Autonomous System Provider Authorization), [draft-ietf-sidrops-aspa-profile-02](#) & [draft-ietf-sidrops-aspa-verification-04](#)
- Deployment
 - Requirements for RPKI Relying Parties, [draft-ietf-sidrops-rp-06](#)
 - RPKI-Based ROV on Export, [draft-ietf-sidrops-ov-egress-04](#)
- Operation
 - The Use of Maxlength in the RPKI, [draft-ietf-sidrops-rpkimaxlen-04](#)
 - BGPsec Validation Signaling, [draft-ietf-sidrops-bgpsec-validation-signaling-03](#)
 - Timing Parameters in the RPKI-Based ROV Supply Chain, [draft-ietf-sidrops-rpki-rov-timing-00](#)
 - RPKI Repository Requirements, [draft-ietf-sidrops-deprecate-rsync-00](#)

WG Items

There is something you might also want to notice.

- Distributing validated cache
 - To define a mechanism called "RPKI validated cache Update in SLURM [RFC 8416] over HTTPs (RUSH)", for the use of SLURM in updating RPKI cache data over HTTP [RFC7540] using HTTPs [RFC2818].
 - <https://tools.ietf.org/html/draft-madi-sidrops-rush-02>

Individual Submissions

Two RFCs from SIDROPS are coming.

Network Working Group
Internet-Draft
Updates: 6811 (if approved)
Intended status: Standards Track
Expires: October 10, 2020

Internet Initiative Japan & Arrcus
R. Bush
R. Volk
Deutsche Telekom
J. Heitz
Cisco
April 8, 2020

BGP RPKI-Based Origin Validation on Export
draft-ietf-sidrops-ov-egress-04

Abstract

A BGP speaker may perform RPKI origin validation not only on routes received from BGP neighbors and routes that are redistributed from other routing protocols, but also on routes it sends to BGP neighbors. For egress policy, it is important that the classification uses the 'effective origin AS' of the processed route, which may specifically be altered by the commonly available knobs such as removing private ASs, confederation handling, and other modifications of the origin AS. This document updates [RFC6811].

AUTH 48 to be RFC 8893

Internet Engineering Task Force (IETF)
Request for Comments: 8897
Category: Informational
ISSN: 2070-1721

D. Ma
ZDNS
S. Kent
Independent
September 2020

Requirements for Resource Public Key Infrastructure (RPKI) Relying Parties

Abstract

This document provides a single reference point for requirements for Relying Party (RP) software for use in the Resource Public Key Infrastructure (RPKI). It cites requirements that appear in several RPKI RFCs, making it easier for implementers to become aware of these requirements. Over time, this RFC will be updated to reflect changes to the requirements and guidance specified in the RFCs discussed herein.

RFC 8897

IETF SIDROPS will be busy as the RPKI is being widely adopted.

- To solicit input from increasing number of operators to identify issues with interaction with the non-SIDR-aware/SIDR-aware Internet, and to determine solutions or workarounds to those issues, as the critical mass of RPKI deployment is being reached.
- To design RPKI deployment models that fit into the evolution of networking technologies and architecture.
- To seek countermeasures to safeguard the RPKI, which has become a globally critical infrastructure of routing control.

Thanks.