Network Working Group Internet-Draft

Intended status: Standards Track

Expires: December 31, 2012

R. Bush
Internet Initiative Japan
R. Austein
Dragon Research Labs
K. Patel
Cisco Systems
H. Gredler
Juniper Networks, Inc.
M. Waehlisch
FU Berlin
July 2012

# RPKI Router Implementation Report draft-ietf-sidr-rpki-rtr-impl-01

#### Abstract

This document provides an implementation report for RPKI Router protocol as defined in [I-D.ietf-sidr-rpki-rtr]. The editor did not verify the accuracy of the information provided by respondents or by any alternative means. The respondents are experts with the implementations they reported on, and their responses are considered authoritative for the implementations for which their responses represent. Respondents were asked to only use the YES answer if the feature had at least been tested in the lab.

#### Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in RFC 2119 [RFC2119] only when they appear in all upper case. They may also appear in lower or mixed case as English words, without any normative meaning.

#### Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of  $\underline{\text{BCP }78}$  and  $\underline{\text{BCP }79}.$ 

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 <a href="http://datatracker.ietf.org/drafts/current/">http://datatracker.ietf.org/drafts/current/</a>.

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 December 31, 2012.

#### Copyright Notice

Copyright (c) 2012 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to <a href="BCP 78">BCP 78</a> and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/ license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

#### Table of Contents

<u>1</u> .	Intro	duction				2
<u>2</u> .	Imple	ementation Forms				3
<u>3</u> .	Proto	ocol Data Units				3
<u>4</u> .	Proto	ocol Sequence				4
<u>5</u> .	Proto	ocol Transport				5
<u>6</u> .	Error	Codes				5
<u>7</u> .	Incre	emental Updates Support				6
<u>8</u> .	Sessi	on ID Support				6
<u>9</u> .	Incre	emental Session Startup Support				7
<u> 10</u> .	Inter	operable Implementations				7
10	<u>9.1</u> .	Cisco Implementation				7
10	<u>9.2</u> .	Juniper Implementation				7
10	<u>3.3</u> .	${\it rpki.net \ Implementation \ . \ . \ . \ . \ . \ .}$				7
10	<u> 9.4</u> .	RIPE NCC Implementation				7
10	<u>9.5</u> .	RTRlib Implementation				7
10	<u>9.6</u> .	BBN RPSTIR Implementation				7
<u>11</u> .	IANA	Considerations				8
<u>12</u> .	Secur	ity considerations				8
<u>13</u> .	Ackno	owledgements				8
<u>14</u> .	Refer	ences				8
Autl	nors'	Addresses				8

# 1. Introduction

In order to formally validate the origin ASs of BGP announcements, routers need a simple but reliable mechanism to receive RPKI [I-D

.ietf-sidr-rpki-rtr] prefix origin data from a trusted cache. The RPKI Router protocol defined in [<u>I-D.ietf-sidr-rpki-rtr</u>] provides a mechanism to deliver validated prefix origin data to routers.

Bush, et al. Expires December 31, 2012 [Page 2]

This document provides an implementation report for the RPKI Router protocol as defined in [I-D.ietf-sidr-rpki-rtr].

The editor did not verify the accuracy of the information provided by respondents or by any alternative means. The respondents are experts with the implementations they reported on, and their responses are considered authoritative for the implementations for which their responses represent. Respondents were asked to only use the YES answer if the feature had at least been tested in the lab.

# **2**. Implementation Forms

Contact and implementation information for person filling out this form:

IOS Name: Keyur Patel, Email: keyupate@cisco.com, Vendor: Cisco
Systems, Inc. Release: IOS

XR Name: Forhad Ahmed, Email:foahmed@cisco.com, Vendor: Cisco Systems, Inc. Release: IOS-XR

JUNOS Name: Hannes Gredler, Email: hannes@juniper.net, Vendor: Juniper Networks, Inc., Release: JUNOS

rpki.net Name: Rob Austein, Email: sra@hactrn.net, Vendor: rpki.net
 project, Release: http://subvert-rpki.hactrn.net/trunk/

NCC Name: Tim Bruijnzeels, Email: tim@ripe.net, Vendor: RIPE NCC Release: RIPE NCC validator-app 2.0.0 <a href="https://certification.ripe.net/content/public-repo/releases/net/ripe/rpki-validator/rpki-validator-app/2.0.0/rpki-validator-app-2.0.0-bin.zip">https://certification.ripe.net/content/public-repo/releases/net/ripe/rpki-validator/rpki-validator-app/2.0.0/rpki-validator-app-2.0.0-bin.zip</a>

RTRlib Name: Fabian Holler, Matthias Waehlisch, Email: waehlisch@ieee.org, Vendor: HAW Hamburg, FU Berlin, RTRlib project, Release: RTRlib 0.2 <a href="http://rpki.realmv6.org/">http://rpki.realmv6.org/</a>

BBN Name: David Mandelberg, Andrew Chi Email: dmandelb@bbn.com, achi@bbn.com, Vendor: Raytheon/BBN Technologies, Release: RPSTIR 0.2 http://sourceforge.net/projects/rpstir/

# 3. Protocol Data Units

Does the implementation support Protocol Data Units (PDUs) as described in Section 5 of [I-D.ietf-sidr-rpki-rtr]?

Bush, et al. Expires December 31, 2012

[Page 3]

+	<b></b>	<b>⊦</b>				+	++
!!!	IOS	XR	JUNOS		NCC	RTR-	BBN
			_	.net	_	lib	
l Rcv.	YES	YES	YES	YES	UNIT	YES	SYS
Serial					TEST		TEST
Notify		i					
Snd.	NO	NO I	NO I	YES	YES	I NO	YES
Serial	İ	i i					i i
Notify	İ	i i	İ				
Rcv.	l NO	NO	NO	YES	YES	l NO	YES
Serial		ĺ	ĺ	ĺ			
Query							
Snd.	YES	YES	YES	YES	UNIT	YES	SYS
Serial					TEST		TEST
Query							
Rcv. Reset	NO NO	NO	NO	YES	YES	l NO	YES
Query							
Snd. Reset	YES	YES	YES	YES	UNIT	YES	SYS
Query					TEST		TEST
Rcv. Cache	YES	YES	YES	YES	UNIT	YES	SYS
Resp.					TEST		TEST
Snd. Cache	NO NO	NO	NO	YES	YES	l NO	YES
Resp.							
Rcv. IPv4	YES	YES	YES	YES	UNIT	YES	SYS
Prefix					TEST		TEST
Snd. IPv4	l NO	NO	NO	YES	YES	l NO	YES
Prefix			\ \ \	\			
Rcv. IPv6	YES	YES	YES	YES	UNIT	YES	SYS
Prefix				\/=0	TEST		TEST
Snd. IPv6	NO NO	NO	NO	YES	YES	l NO	YES
Prefix	   VEC		\ \/FC	VEC	LINITT	 	
Rcv. End	YES	YES	YES	YES	UNIT	YES	SYS
of Data	l NO		NO	VEC	TEST	l NO	TEST
Snd. End     of Data	NO NO	NO   	NO	YES	YES	l NO	YES
Rcv. Cache	l   YES	l YES	YES	YES	   UNIT	I   YES	I I SYS
Reset	l IES	l IES	163	163	TEST	l IES	313     TEST
Snd. Cache	I I NO	l NO I	NO	YES	YES	I I NO	YES
Reset	140	NO   	140	120	125	140	120
Rcv. Error	l YES	ı yes	NO~1	YES	YES	ı   YES	ı ı   YES
Report	U	,0   		0	0	, . <u></u>	,o   
Snd. Error	l YES	NO	NO	YES	YES	ı   YES	ı YES
Report		 		0		, . <u>-</u> -	
+			· 	י ++	, 	+	+

1) No, Error PDU gets silently ignored

# 4. Protocol Sequence

Does RPKI Router protocol implementation follow the four protocol sequences as outlined in Section 6 of [I-D.ietf-sidr-rpki-rtr]?

Bush, et al. Expires December 31, 2012 [Page 4]

S1: Start or Restart

S2: Typical Exchange

S3: Generation of Incremental Updates Sequence

S4: Receipt of Incremental Updates Sequence

S5: Generation of Cache has No data Sequence

++	+	+		+	+	-++
IOS	XR	JUNOS	rpki.net	NCC	RTRlib	BBN
++	+	+		+	+	-++
S1   YES	YES	YES	YES	YES	YES	YES
S2   YES	YES	YES	YES	NO~1	YES	YES
S3   NO	NO	NO	YES	NO	YES	YES
S4   YES	YES	YES	YES	NO	YES	NO
S5   NO	NO	NO	YES	YES	YES	YES
++	+	+		+	+	-++

1) NO, we always respond as described in 6.3 of [I-D.ietf-sidr-rpki-rtr]

# 5. Protocol Transport

Does RPKI Router protocol implementation support different protocol transport mechanism outlined in <u>Section 7</u> of [I-D.ietf-sidr-rpki-rtr]?

+		+ -		- + -		+-		+		- + -	+		+		+
		•		•		•		•	•	•			•		•
+		+ -		- + -		+-		+		- + -	+		+		+
	SSH		NO		YES		NO		YES		NO	YES		YES~1	
ĺ	TLS	ĺ	NO	Ì	NO	ĺ	NO	Ì	NO	Ì	NO	NO	ĺ	NO	Ì
	TCP		YES		YES		YES		YES		YES	YES		YES	
	TCP-MD5		NO		NO		NO		NO		NO	NO		NO	
	TCP-A0		NO		NO		NO		NO		NO	NO		NO	
+		+.		+.		+.		+		_ + .	4		+		. +

1) Yes, using netcat as the ssh subsystem to connect to the RTR server on localhost via TCP. This is currently untested.

#### 6. Error Codes

Does RPKI Router protocol implementation support different protocol error codes outlined in Section 10 of [I-D.ietf-sidr-rpki-rtr]?

Bush, et al. Expires December 31, 2012

[Page 5]

++		<b></b>	-+	+	++
IOS   XR	JUNOS	rpki.net	NCC	RTRlib	BBN
++			-+	+ ·	++
Rcv.0   YES   YES	NO	YES	YES	YES	YES
Snd.0   YES   YES	NO	YES	YES	YES	YES
Rcv.1   YES   YES	NO	YES	YES	YES	YES
Snd.1   YES   YES	NO	YES	YES	YES	YES
Rcv.2   YES   YES	NO	YES	N/A	YES	YES
Snd.2   YES   YES	NO	YES	YES	N/A	YES
Rcv.3   YES   YES	NO	YES	N/A	YES	YES
Snd.3   NO   NO	NO	YES	YES	l NO	YES
Rcv.4   YES   YES	NO	YES	YES	YES	YES
Snd.4   YES   YES	NO	YES	YES	YES	YES
Rcv.5   YES   YES	NO	YES	YES	YES	YES
Snd.5   YES   YES	NO	YES	YES	YES	YES
Rcv.6   NO   NO	NO	YES	YES~1	N/A	YES
Snd.6   YES   YES	NO	NO	N/A	YES	SYS TEST
Rcv.7   NO   NO	NO	YES	YES~1	N/A	YES
Snd.7   YES   YES	NO	NO	N/A	YES	SYS TEST
++		<b></b>	-+	+	++

1) YES, but... fatal, so connection is dropped, but cache does not conclude it's inconsistent

# 7. Incremental Updates Support

RPKI Router protocol does support Incremental Updates defined in Section 4 of [I-D.ietf-sidr-rpki-rtr].

+	+	++		++
IOS   XR   JUNOS				
NO   NO   YES~1	YES	NO	YES	YES

1) YES, receive side support

#### 8. Session ID Support

Session ID is used to indicate that the cache server may have restarted and that the incremental restart may not be possible.

Does RPKI Router protocol implementation support Session ID procedures outlined in Section 5.10 of [I-D.ietf-sidr-rpki-rtr]?

+		-+-		+-		+ -		+		+ -		+-		+
	IOS		XR		JUNOS		rpki.net		NCC		RTRlib		BBN	
+		-+-		+-		+ -		+		+ -		+-		+
ı	YES	1	YES	Τ	YES	Ι	YES	Ι	NO~1	ī	YES	ı	YES	Ι

+----+

1) NO, using random, but will FIX

Bush, et al. Expires December 31, 2012 [Page 6]

#### 9. Incremental Session Startup Support

RPKI Router protocol does support Incremental session startups with Serial Number and Session ID defined in the protocol. Does RPKI Router protocol implementation support Incremental Session Startup Support as defined in section 5.4 of [I-D.ietf-sidr-rpki-rtr].

+		-+-		+		+		+-		+		+-	+
	IOS		XR		JUNOS		rpki.net		NCC		RTRlib		BBN
+		-+-		+-		+		+-		+		+-	+
	YES	1	YES		YES		YES		NO		YES		YES
+		-+-		+ -		+ -		+ -		+		+-	+

### 10. Interoperable Implementations

List other implementations that you have tested interoperability of RPKI Router Implementation.

#### 10.1. Cisco Implementation

Cisco: The Cisco IOS and IOS-XR implementation should be interoperable with other vendor RPKI Router Protocol implementations. In particular we have tested our interoperability with rpki.net's RPKI Router implementation.

# 10.2. Juniper Implementation

Juniper: The Juniper Networks, Inc. JUNOS implementation should be interoperable with other vendor RPKI Router Protocol implementations. In particular we have tested our interoperability with rpki.net's and NCCs RPKI Router Cache implementation.

#### 10.3. rpki.net Implementation

rpki.net: The rpki.net implementation should operate with other rpkirtr implementations. In particular, we have tested our interoperability with Cisco IOS, Cisco IOS-XR, and Juniper.

## 10.4. RIPE NCC Implementation

RIPE NCC: The RIPE NCC validator has been tested by us with other rpki-rtr implementations. In particular we have tested with RTRLib and CISCO IOS. We received positive feedback from close contacts testing our validator with JUNOS and Quagga.

#### 10.5. RTRlib Implementation

RTRlib: The RTRlib has been tested by us with other rpki-rtr implementations. In particular, we have tested with rtr-origin from

rpki.net and RIPE NCC Validator.

# **10.6**. BBN RPSTIR Implementation

Bush, et al. Expires December 31, 2012

[Page 7]

BBN RPSTIR: We have not yet tested with any other implementations.

#### 11. IANA Considerations

This document makes no request of IANA.

Note to RFC Editor: this section may be removed on publication as an RFC.

#### 12. Security considerations

No new security issues are introduced to the RPKI Router protocol defined in [I-D.ietf-sidr-rpki-rtr].

# 13. Acknowledgements

TBD....

#### 14. References

```
[I-D.ietf-sidr-rpki-rtr]

Bush, R. and R. Austein, "The RPKI/Router Protocol",

Internet-Draft <a href="mailto:draft-ietf-sidr-rpki-rtr-26">draft-ietf-sidr-rpki-rtr-26</a>, February 2012.
```

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", <u>BCP 14</u>, <u>RFC 2119</u>, March 1997.

Authors' Addresses

Randy Bush Internet Initiative Japan 5147 Crystal Springs Bainbridge Island, Washington 98110 US

Email: randy@psg.com

Rob Austein Dragon Research Labs

Email: sra@hactrn.net

Keyur Patel Cisco Systems 170 West Tasman Drive San Jose, CA 95134 US Bush, et al. Expires December 31, 2012

[Page 8]

Hannes Gredler Juniper Networks, Inc. 1194 N. Mathilda Ave. Sunnyvale, CA 94089 US

Email: hannes@juniper.net

Matthias Waehlisch FU Berlin Takustr. 9 Berlin 14195 Germany

Email: waehlisch@ieee.org

URI: <a href="http://www.inf.fu-berlin.de/~waehl">http://www.inf.fu-berlin.de/~waehl</a>