Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: October 11, 2013

R. Bush
Internet Initiative Japan
K. Patel
Cisco Systems
S. Turner
IECA, Inc.

April 09, 2013

Router Key PDU for RPKI-Router Protocol
draft-ymbk-rpki-rtr-keys-01

Abstract

The RPKI/Router Protocol v0 is specified to carry the PDUs necessary for RPKI-based Origin Validation. For BGPsec Path Validation, the routers also need data extracted from BGPsec Router Certificates. This document adds a PDU to the RPKI/Router Protocol to carry those data.

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 http://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 October 11, 2013.

Table of Contents

1. Introduction

The RPKI/Router Protocol v0, see [RFC6810], defines the PDUs necessary for RPKI-based Origin Validation. For BGPsec Path Validation ([I-D.ietf-sidr-bgpsec-protocol]), the routers also need data extracted from BGPsec Router Certificates which are described in Section 3.1 of [I-D.ietf-sidr-bgpsec-pki-profiles]. This document adds a PDU to the RPKI/Router Protocol to carry those data.

This is a temporary design document intended to work out the design of the PDU. How the RPKI/Router protocol specification is enhanced to include this PDU will be dealt with later.

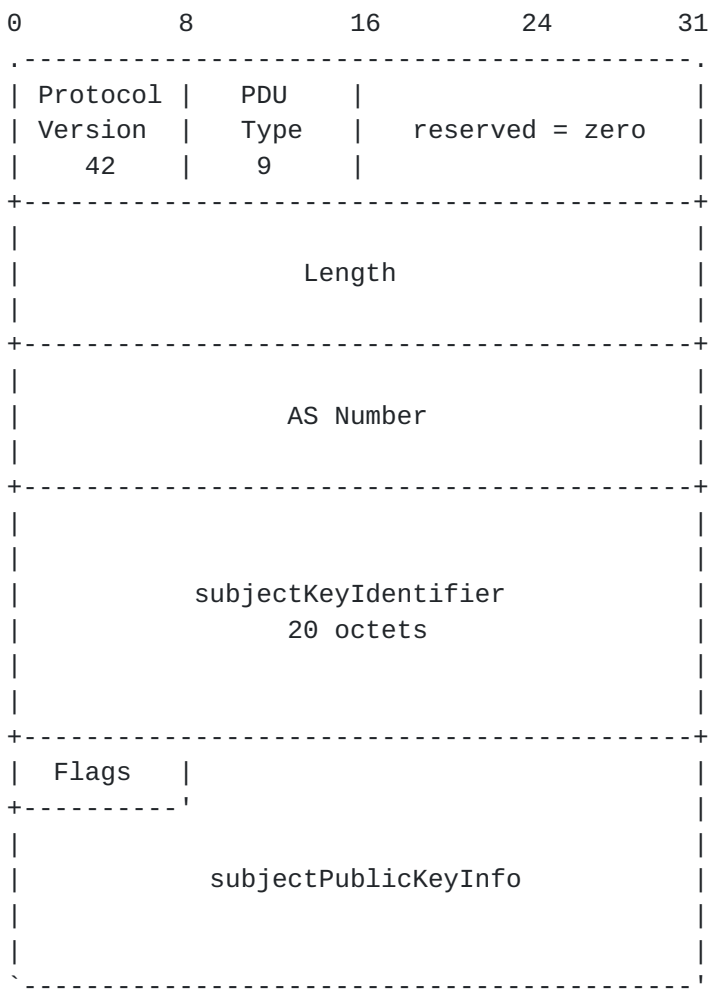
2. The Data Needed by the Router

As in the RPKI/Router protocol v0, very little of the data in the RPKI is actually needed by the router. Only those data required by the router are carried in this PDU. In addition to the normal boilerplate fields of an RPKI/Router PDU (Protocol Version, Serial Number, and Flags), the Router Key PDU has the following fields:

PDU Type: An eight-bit unsigned integer with the value 9.
AS Number: The 4-byte Autonomous System Number (AS or ASN) of the router extracted from [I-D.ietf-sidr-bgpsec-pki-profiles] Section 3.1.1.1 (sic).
Subject Key Identifier: The 20 octet subjectKeyIdentifier (SKI) as described in Section 4.8.2 of [RFC6487].
Subject Public Key Info: The router's subjectPublicKeyInfo (SPKI) as described in section 3.1 of [I-D.ietf-sidr-bgpsec-algs]. The first two octets of the SPKI are the Tag (currently 0x30) and the

Length (currently 0x59) of the SPKI. They are followed by an algorithmIdentifier and a subjectPublicKey.

3. The PDU Format



4. IANA Considerations

This document requests the IANA to modify the registry for tuples of Protocol Version / PDU Type, to add the PDU Type 9 as follows:

Protocol Version	PDU Type
0	9 - Router Key

5. References

5.1. Normative References

[I-D.ietf-sidr-bgpsec-algs]
Turner, S., "BGP Algorithms, Key Formats, & Signature Formats", draft-ietf-sidr-bgpsec-algs-04 (work in progress), March 2013.

[I-D.ietf-sidr-bgpsec-pki-profiles]
Reynolds, M., Turner, S., and S. Kent, "A Profile for BGPSEC Router Certificates, Certificate Revocation Lists, and Certification Requests", draft-ietf-sidr-bgpsec-pki-profiles-04 (work in progress), October 2012.

[RFC6487] Huston, G., Michaelson, G., and R. Loomans, "A Profile for X.509 PKIX Resource Certificates", RFC 6487, February 2012.

[RFC6810] Bush, R. and R. Austein, "The Resource Public Key Infrastructure (RPKI) to Router Protocol", RFC 6810, January 2013.

5.2. Informative References

[I-D.ietf-sidr-bgpsec-protocol]
Lepinski, M., "BGPSEC Protocol Specification", draft-ietf-sidr-bgpsec-protocol-07 (work in progress), February 2013.

Authors' Addresses

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

Email: randy@psg.com

Keyur Patel
Cisco Systems
170 W. Tasman Drive
San Jose, CA 95134
USA

Email: keyupate@cisco.com

Sean Turner
IECA, Inc.
3057 Nutley Street, Suite 106
Fairfax, Virginia 22031
US

Email: turners@ieca.com