

Network Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: November 12, 2011

T. Manderson  
L. Vegoda  
ICANN  
S. Kent  
BBN  
May 11, 2011

RPKI Objects issued by IANA  
draft-ietf-sidr-iana-objects-03.txt

## Abstract

This document provides specific direction to IANA as to the Resource Public Key Infrastructure (RPKI) objects it should issue.

## 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 November 12, 2011.

## Copyright Notice

Copyright (c) 2011 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) 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

<a href="#">1.</a>	Requirements Notation . . . . .	<a href="#">3</a>
<a href="#">2.</a>	Introduction . . . . .	<a href="#">4</a>
<a href="#">3.</a>	Required Reading . . . . .	<a href="#">5</a>
<a href="#">4.</a>	Definitions . . . . .	<a href="#">6</a>
<a href="#">5.</a>	Reserved Resources . . . . .	<a href="#">7</a>
<a href="#">6.</a>	Unallocated Resources . . . . .	<a href="#">8</a>
<a href="#">7.</a>	Special Purpose Registry Resources . . . . .	<a href="#">9</a>
<a href="#">8.</a>	Multicast . . . . .	<a href="#">10</a>
<a href="#">9.</a>	Informational Objects . . . . .	<a href="#">11</a>
<a href="#">10.</a>	Certificates and CRLs . . . . .	<a href="#">12</a>
<a href="#">11.</a>	IANA Considerations . . . . .	<a href="#">13</a>
<a href="#">12.</a>	Security Considerations . . . . .	<a href="#">14</a>
<a href="#">13.</a>	Acknowledgements . . . . .	<a href="#">15</a>
<a href="#">14.</a>	References . . . . .	<a href="#">16</a>
<a href="#">14.1.</a>	Normative References . . . . .	<a href="#">16</a>
<a href="#">14.2.</a>	Informative References . . . . .	<a href="#">16</a>
<a href="#">Appendix A.</a>	IANA Reserved IPv4 Address Blocks . . . . .	<a href="#">19</a>
<a href="#">Appendix B.</a>	IANA Reserved IPv6 Address Blocks . . . . .	<a href="#">20</a>
	Authors' Addresses . . . . .	<a href="#">22</a>

## 1. Requirements Notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [[RFC2119](#)].

## 2. Introduction

An Infrastructure to Support Secure Internet Routing [[I-D.ietf-sidr-arch](#)] directs IANA [[RFC2860](#)] to issue Resource Public Key Infrastructure (RPKI) objects for which it is authoritative. This document describes the objects IANA will issue. If IANA is directed to issue additional RPKI objects in future, this document will be revised and a new version issued.

The signed objects described here that IANA will issue are the unallocated, reserved, special use IPv4 and IPv6 address blocks, and the unallocated and reserved Autonomous System numbers. These number resources are managed by IANA for the IETF, and thus IANA bears the responsibility of issuing the corresponding RPKI objects. The reader is encouraged to consider the technical effects on the public routing system of the signed object issuance proposed for IANA in this document.

This document does not deal with BGP [[RFC4271](#)] routing systems as those are under the policy controls of the organizations that operate them. Readers are directed to Local Trust Anchor Management for the Resource Public Key Infrastructure [[I-D.ietf-sidr-ltamgmt](#)] for a description of how to locally override IANA issued objects, e.g. to enable use of unallocated, reserved, and special use IPv4 and IPv6 address blocks in a local context.

The direction to IANA contained herein follows the ideal that it should represent the ideal technical behavior for registry, and related registry, actions.

### 3. Required Reading

Readers should be familiar with the RPKI, the RPKI Repository Structure, and the various RPKI objects, uses and interpretations described in the following: [[I-D.ietf-sidr-arch](#)], [[I-D.ietf-sidr-res-certs](#)], [[I-D.ietf-sidr-roa-format](#)], [[I-D.ietf-sidr-ghostbusters](#)], [[I-D.ietf-sidr-ltamgmt](#)], [[I-D.ietf-sidr-roa-validation](#)], [[I-D.ietf-sidr-usecases](#)], [[I-D.ietf-sidr-cp](#)], and [[I-D.ietf-sidr-rpki-manifests](#)].

NOTE: The addresses used in this document are not example addresses therefore they are not compliant with [[RFC3849](#)], [[RFC5735](#)], and [[RFC5771](#)]. This is intentional as the practices described in this document are directed to specific instances of real world addresses.

#### [4.](#) Definitions

Internet Number Resources (INR): The number identifiers for IPv4 [[RFC0791](#)] and IPv6 [[RFC2460](#)] addresses, and for Autonomous Systems.

IANA: Internet Assigned Numbers Authority (a traditional name, used here to refer to the technical team making and publishing the assignments of Internet protocol technical parameters). The technical team of IANA is currently a part of ICANN [[RFC2860](#)].

RPKI: Resource Public Key Infrastructure. A Public Key Infrastructure designed to provide a secure basis for assertions about holdings of Internet numeric resources. Certificates issued under the RPKI contain additional attributes that identify IPv4, IPv6, and Autonomous System Number (ASN) resources

[\[I-D.ietf-sidr-arch\]](#).

ROA: Route Origination Authorization. A ROA is an RPKI object that enables the holder of the address prefix to specify an AS that is permitted to originate (in BGP) routes for that prefix [\[I-D.ietf-sidr-roa-format\]](#).

AS0 ROA: A ROA containing a value of 0 in the ASID field. Validation of Route Origination using the Resource Certificate PKI and ROAs [\[I-D.ietf-sidr-roa-validation\]](#) states "A ROA with a subject of AS0 (AS0-ROA) is an attestation by the holder of a prefix that the prefix described in the ROA, and any more specific prefix, should not be used in a routing context."

"Not intended to be (publicly) routed": This phrase refers to prefixes that are not meant to be represented in the global Internet routing table (for example 192.168/16, [\[RFC1918\]](#)).

## [5.](#) Reserved Resources

Reserved IPv4 and IPv6 resources are held back for various reasons by IETF action. Generally such resources are not intended to be globally routed. An example of such a reservation is 127.0.0.0/8 [\[RFC5735\]](#). See [Appendix A](#) (Appendix A) and [B](#) (Appendix B) for IANA reserved resources.

IANA SHOULD issue an AS0 ROA for all reserved IPv4 and IPv6 resources not intended to be routed. The selection of the [\[RFC2119\]](#) terminology is intentional as there may be situations where the AS0 ROA is removed or not issued prior to an IANA registry action. It is not appropriate to place IANA into a situation where, through normal internal operations, its behavior contradicts IETF standards.

There are a small number of reserved resources that are intended to be routed, for example 192.88.99.0/24 [\[RFC3068\]](#). See [Appendix A](#) (Appendix A) and B (Appendix B) for IANA reserved resources.

IANA MUST NOT issue any ROAs (AS0 or otherwise) for reserved resources that are expected to be globally routed.

Internet Number Resources that have not yet been allocated for special purposes [[RFC5736](#)], to Regional Internet Registries (RIRs), or to others are considered as not intended to be globally routed.

IANA SHOULD issue an AS0 ROA for all Unallocated Resources. The selection of the [[RFC2119](#)] terminology is intentional as there may be situations where the AS0 ROA is removed or not issued prior to an IANA registry action. It is not appropriate to place IANA into a situation where, through normal internal operations, its behavior contradicts IETF standards.

## 7. Special Purpose Registry Resources

Special Registry Resources [[RFC5736](#)] fall into one of two categories in terms of routing. Either the resource is intended to be seen in the global Internet routing table in some fashion, or it isn't. An example of a special purpose registry INR that is intended for global routing is 2001:0000::/32 [[RFC4380](#)]. An example of an INR not intended to be seen would be 2001:002::/48 [[RFC5180](#)].

IANA MUST NOT issue any ROAs (AS0 or otherwise) for Special Purpose Registry Resources that are intended to be globally routed.

IANA SHOULD issue an AS0 ROA for Special Purpose Registry Resources that are not intended to be globally routed.

## [8.](#) Multicast

Within the IPv4 Multicast [[RFC5771](#)] and IPv6 Multicast [[RFC4291](#)] registries there are a number of Multicast registrations that are not intended to be globally routed.

IANA MUST issue an AS0 ROA covering the following IPv4 and IPv6 multicast INRs:

### IPv4:

- Local Network Control Block  
224.0.0.0 - 224.0.0.255 (224.0.0/24)
- IANA Reserved portions of RESERVED  
224.1.0.0-224.1.255.255 (224.1/16)
- RESERVED  
224.5.0.0-224.251.255.255 (251 /16s)  
225.0.0.0-231.255.255.255 (7 /8s)

### IPv6:

- Node-Local Scope Multicast Addresses
- Link-Local Scope Multicast Addresses

IANA MUST NOT issue any ROAs (AS0 or otherwise) for any other multicast addresses unless directed by an IESG approved standards track document with an appropriate IANA Considerations section.

## 9. Informational Objects

One informational object that can exist at a publication point of an RPKI repository is the Ghostbusters Record [[I-D.ietf-sidr-ghostbusters](#)].

IANA MUST issue a ghostbusters object appropriate in content for the resources IANA maintains.

## 10. Certificates and CRLs

Before IANA can issue a ROA it MUST first establish an RPKI Certification Authority (CA) that covers unallocated, reserved, and special use INRs. A CA that covers these INRs MUST contain contain [RFC 3379](#) extensions [[RFC3779](#)] for those corresponding number resources in its Certificate. This CA MUST issue single-use End Entity (EE) certificates for each ROA that it generates. The EE certificate will conform to the Resource Certificate Profile [[I-D.ietf-sidr-res-certs](#)] and the additional constraints specified in [[I-D.ietf-sidr-roa-format](#)]. IANA MUST maintain a publication point for this CA's use and MUST publish manifests [[I-D.ietf-sidr-rpki-manifests](#)] (with its corresponding EE certificate) for this publication point. IANA MUST issue a Certificate Revocation List (CRL) under this CA certificate for the EE certificates noted above. All objects issued by this CA will conform to the RPKI Certificate Policy [[I-D.ietf-sidr-cp](#)].

## [11.](#) IANA Considerations

This document directs IANA to issue, or refrain from issuing, the specific RPKI objects described here for the current set of reserved, unallocated, and special registry Internet Number Resources. Further IANA MUST notify all other INR registries that RPKI objects have been issued for the Internet Number Resources described in this document to avoid the potential for issuance of duplicate objects that might confuse relying parties.

## [12.](#) Security Considerations

This document does not alter the security profile of the RPKI from that already discussed in SDR-WG documents.

### [13.](#) Acknowledgements

The authors acknowledge Dave Meyer for helpful direction with regard to multicast assignments.



## [14.](#) References

### [14.1.](#) Normative References

[I-D.ietf-sidr-arch]

Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", [draft-ietf-sidr-arch-12](#) (work in progress), February 2011.

[I-D.ietf-sidr-cp]

Kent, S., Kong, D., Seo, K., and R. Watro, "Certificate Policy (CP) for the Resource PKI (RPKI)", [draft-ietf-sidr-cp-17](#) (work in progress), April 2011.

[I-D.ietf-sidr-ghostbusters]

Bush, R., "The RPKI Ghostbusters Record", [draft-ietf-sidr-ghostbusters-03](#) (work in progress), March 2011.

[I-D.ietf-sidr-res-certs]

Huston, G., Michaelson, G., and R. Loomans, "A Profile for X.509 PKIX Resource Certificates", [draft-ietf-sidr-res-certs-22](#) (work in progress), May 2011.

[I-D.ietf-sidr-roa-format]

Lepinski, M., Kent, S., and D. Kong, "A Profile for Route Origin Authorizations (ROAs)", [draft-ietf-sidr-roa-format-12](#) (work in progress), May 2011.

[I-D.ietf-sidr-roa-validation]

Huston, G. and G. Michaelson, "Validation of Route Origination using the Resource Certificate PKI and ROAs", [draft-ietf-sidr-roa-validation-10](#) (work in progress), November 2010.

[I-D.ietf-sidr-rpki-manifests]

Austein, R., Huston, G., Kent, S., and M. Lepinski, "Manifests for the Resource Public Key Infrastructure", [draft-ietf-sidr-rpki-manifests-11](#) (work in progress), May 2011.

### [14.2.](#) Informative References

[I-D.ietf-sidr-ltamgmt]

Kent, S. and M. Reynolds, "Local Trust Anchor Management for the Resource Public Key Infrastructure",

November 2010.

[I-D.ietf-sidr-usecases]

Manderson, T., Sriram, K., and R. White, "Use Cases and interpretation of RPKI objects for issuers and relying parties", [draft-ietf-sidr-usecases-01](#) (work in progress), December 2010.

[RFC0791] Postel, J., "Internet Protocol", STD 5, [RFC 791](#), September 1981.

[RFC0919] Mogul, J., "Broadcasting Internet Datagrams", STD 5, [RFC 919](#), October 1984.

[RFC0922] Mogul, J., "Broadcasting Internet datagrams in the presence of subnets", STD 5, [RFC 922](#), October 1984.

[RFC1112] Deering, S., "Host extensions for IP multicasting", STD 5, [RFC 1112](#), August 1989.

[RFC1122] Braden, R., "Requirements for Internet Hosts - Communication Layers", STD 3, [RFC 1122](#), October 1989.

[RFC1918] Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G., and E. Lear, "Address Allocation for Private Internets", [BCP 5](#), [RFC 1918](#), February 1996.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", [RFC 2460](#), December 1998.

[RFC2544] Bradner, S. and J. McQuaid, "Benchmarking Methodology for Network Interconnect Devices", [RFC 2544](#), March 1999.

[RFC2860] Carpenter, B., Baker, F., and M. Roberts, "Memorandum of Understanding Concerning the Technical Work of the Internet Assigned Numbers Authority", [RFC 2860](#), June 2000.

- [RFC3068] Huitema, C., "An Anycast Prefix for 6to4 Relay Routers", [RFC 3068](#), June 2001.
- [RFC3779] Lynn, C., Kent, S., and K. Seo, "X.509 Extensions for IP Addresses and AS Identifiers", [RFC 3779](#), June 2004.
- [RFC3849] Huston, G., Lord, A., and P. Smith, "IPv6 Address Prefix Reserved for Documentation", [RFC 3849](#), July 2004.

Manderson, et al.

Expires November 12, 2011

[Page 17]

---

Internet-Draft

IANA RPKI Objects

May 2011

- [RFC3879] Huitema, C. and B. Carpenter, "Deprecating Site Local Addresses", [RFC 3879](#), September 2004.
- [RFC3927] Cheshire, S., Aboba, B., and E. Guttman, "Dynamic Configuration of IPv4 Link-Local Addresses", [RFC 3927](#), May 2005.
- [RFC4271] Rekhter, Y., Li, T., and S. Hares, "A Border Gateway Protocol 4 (BGP-4)", [RFC 4271](#), January 2006.
- [RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", [RFC 4291](#), February 2006.
- [RFC4380] Huitema, C., "Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)", [RFC 4380](#), February 2006.
- [RFC4843] Nikander, P., Laganier, J., and F. Dupont, "An IPv6 Prefix for Overlay Routable Cryptographic Hash Identifiers (ORCHID)", [RFC 4843](#), April 2007.
- [RFC5180] Popoviciu, C., Hamza, A., Van de Velde, G., and D. Dugatkin, "IPv6 Benchmarking Methodology for Network Interconnect Devices", [RFC 5180](#), May 2008.
- [RFC5735] Cotton, M. and L. Vegoda, "Special Use IPv4 Addresses", [BCP 153](#), [RFC 5735](#), January 2010.
- [RFC5736] Huston, G., Cotton, M., and L. Vegoda, "IANA IPv4 Special Purpose Address Registry", [RFC 5736](#), January 2010.
- [RFC5737] Arkko, J., Cotton, M., and L. Vegoda, "IPv4 Address Blocks Reserved for Documentation", [RFC 5737](#), January 2010.

[RFC5771] Cotton, M., Vegoda, L., and D. Meyer, "IANA Guidelines for IPv4 Multicast Address Assignments", [BCP 51](#), [RFC 5771](#), March 2010.

Manderson, et al.

Expires November 12, 2011

[Page 18]

Internet-Draft

IANA RPKI Objects

May 2011

#### [Appendix A](#). IANA Reserved IPv4 Address Blocks

This list of Address Space and RFCs was correct at the time of writing

IPv4 Address Blocks and the RFCs which direct IANA to Reserve them

Prefix	RFC	TBR
0.0.0.0/8	<a href="#">RFC1122, Section 3.2.1.3</a>	No
10.0.0.0/8	<a href="#">RFC1918</a>	No
127.0.0.0/8	<a href="#">RFC1122, Section 3.2.1.3</a>	No
169.254.0.0/16	<a href="#">RFC3927</a>	No
172.16.0.0/12	<a href="#">RFC1918</a>	No
192.0.0.0/24	<a href="#">RFC5736</a>	Various
192.0.2.0/24	<a href="#">RFC5737</a>	No
192.88.99.0/24	<a href="#">RFC3068</a>	Yes

192.168.0.0/16	<a href="#">RFC1918</a>	No
198.18.0.0/15	<a href="#">RFC2544</a>	No
198.51.100.0/24	<a href="#">RFC5737</a>	No
203.0.113.0/24	<a href="#">RFC5737</a>	No
224.0.0.0/4	<a href="#">RFC5771</a>	No
240.0.0.0/4	<a href="#">RFC1112, Section 4</a>	No
255.255.255.255/32	<a href="#">RFC919, Section 7</a> and <a href="#">RFC922, Section 7</a>	No

TBR: To Be Routed, the intention of the RFC pertaining to the address block.

Table 1

## [Appendix B](#). IANA Reserved IPv6 Address Blocks

This list of Address Space and RFCs was correct at the time of writing

IPv6 Address Blocks and the RFCs which direct IANA to Reserve them

Prefix	RFC	TBR
0000::/8	<a href="#">RFC4291</a>	No
0100::/8	<a href="#">RFC4291</a>	No
0200::/7	<a href="#">RFC4291</a>	No
0400::/6	<a href="#">RFC4291</a>	No
0800::/5	<a href="#">RFC4291</a>	No

1000::/4	<a href="#">RFC4291</a>	No
4000::/3	<a href="#">RFC4291</a>	No
6000::/3	<a href="#">RFC4291</a>	No
8000::/3	<a href="#">RFC4291</a>	No
A000::/3	<a href="#">RFC4291</a>	No
C000::/3	<a href="#">RFC4291</a>	No
E000::/4	<a href="#">RFC4291</a>	No
F000::/5	<a href="#">RFC4291</a>	No
F800::/6	<a href="#">RFC4291</a>	No
FC00::/7	<a href="#">RFC4193</a>	No
FE00::/9	<a href="#">RFC4291</a>	No
FE80::/10	<a href="#">RFC4291</a>	No
FEC0::/10	<a href="#">RFC3879</a>	No
FF00::/8	<a href="#">RFC4291</a>	No

2001:0002::/48	<a href="#">RFC5180</a>	No
2001:10::/28	<a href="#">RFC4843</a>	No

TBR: To Be Routed, the intention of the RFC pertaining to the address block.

Table 2

Internet-Draft IANA RPKI Objects May 2011

Authors' Addresses

Terry Manderson  
ICANN

Email: [terry.manderson@icann.org](mailto:terry.manderson@icann.org)

Leo Vegoda  
ICANN

Email: [leo.vegoda@icann.org](mailto:leo.vegoda@icann.org)

Steve Kent  
BBN

Email: [kent@bbn.com](mailto:kent@bbn.com)