Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: August 20, 2011

T. Manderson
L. Vegoda
ICANN
S. Kent
BBN

February 16, 2011

RPKI Objects issued by IANA
draft-ietf-sidr-iana-objects-01.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 August 20, 2011.

Copyright Notice

Table of Contents

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.

The signed objects described here that IANA will issue are the unallocated, reserved, special use IPv4 and IPv6 address blocks, 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 localized 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 perfect technical behavior in registry, and related registry, actions.

3. Suggested 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 affect 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.

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.

AS0 ROA: 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].

IANA SHOULD issue an AS0 ROA for all reserved IPv4 and IPv6 resources

not intended to be routed.

There are a small number of reserved resources which are intended to be routed, for example 192.88.99.0/24 [RFC3068].

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

6. Unallocated Resources

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 MUST issue an AS0 ROA for all Unallocated Resources.

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 MUST 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.

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 a RPKI Certificate Authority (CA) that covers unallocated, reserved, and special use INRs by containing RFC 3379 extensions [RFC3779] for those corresponding number resources in the CA Certificate. This CA MUST issue single use End Entity (EE) certificates for each ROA. 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 publish manifests [I-D.ietf-sidr-rpki-manifests] (with its corresponding EE certificate). A Certificate Revocation List (CRL) will be issued under this CA certificate. All objects issued by this CA will conform to a published Certificate Policy [I-D.ietf-sidr-cp].

11. IANA Considerations

This document directs IANA to issue, or refrain from issuing, the specific objects described here for the current set of reserved, unallocated, and special registry Internet Number Resources. Further it MUST notify all other INR registries that RPKI objects have been issued for specific Internet Number Resources to avoid duplicates being issued thus reducing the burden on any relying party.

12. Security Considerations

This document does not alter the security profile of the RPKI from that already discussed in SIDR-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-11 (work in progress), September 2010.

[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-16 (work in progress), December 2010.

[I-D.ietf-sidr-ghostbusters]
Bush, R., "The RPKI Ghostbusters Record", draft-ietf-sidr-ghostbusters-00 (work in progress), December 2010.

[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-21 (work in progress), December 2010.

[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-09 (work in progress), November 2010.

[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-09 (work in progress), November 2010.

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

Requirement Levels", BCP 14, RFC 2119, March 1997.

[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.

[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.

[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.

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

14.2. Informative References

[I-D.ietf-sidr-ltamgmt]
Kent, S. and M. Reynolds, "Local Trust Anchor Management for the Resource Public Key Infrastructure", draft-ietf-sidr-ltamgmt-00 (work in progress), 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.

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

Authors' Addresses

Terry Manderson
ICANN

Email: terry.manderson@icann.org

Leo Vegoda
ICANN

Email: leo.vegoda@icann.org

Steve Kent
BBN

Email: kent@bbn.com