Internet Draft
Expires December 23, 1999
draft-ietf-rps-icann-00

Cengiz Alaettinoglu
USC/ISI
Curtis Villamizar
Avici Systems
Ramesh Govindan
USC/ISI
June 23, 1999

RPS ICANN Issues

Status of this Memo:

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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.'

The list of current Internet-Drafts can be accessed at
`<http://www.ietf.org/ietf/1id-abstracts.txt>`

The list of Internet-Draft Shadow Directories can be accessed at
`<http://www.ietf.org/shadow.html>`.

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 RFC 2119.

Abstract

RPS Security [2] requires certain RPSL [1] objects in the IRR to be hierarchically delegated. The set of objects that are at the root of this hierarchy needs to be created and digitally signed by ICANN. This paper presents these seed objects and lists operations required from ICANN.

1 Initial Seed

A public key of ICANN needs to be distributed with the software implementations of Distributed Routing Policy System [3]. An initial set of seed objects are needed to be signed with this key. They are:

```
mntner:        mnt-icann
descr:         icann's maintainer
admin-c:       . . .
tech-c:        . . .
upd-to:        . . .
mnt-nfy:       . . .
auth:          pgpkey-12345
mnt-by:        mnt-icann
referral-by:   mnt-icann
source:        ICANN

key-cert: pgpkey-12345
method: pgp
owner:  . . .
fingerpr: . . .
certif: # this key is for illustration only
+       -----BEGIN PGP PUBLIC KEY BLOCK-----
+       Version: PGP for Personal Privacy 5.0
+
+       mQFCBDZDU98RAwDUmo45DdsS5W8zjTT0wr0MGIxhpdgGEajiwcjUF2EJm/7w7rEt
+       2W0qXqPupF2lrbb8D3keBnIPW8oyvn0tl471yerBeuBsR50U+D039/yFbpcG004F
+       IhYB5TB0rPuUUl8AoP+bUmGP6DudkE+wDgNlcY5UnEBnAwDIB9umMEKK0kDcFy/Q
+       34gLNplxARbNjyIFLDOg/W2qfBb9/RfQLNGfgPWqYz47tIN1rYhErDWDJjjhWkNd
+       Fb7sARhqCotnkJrJ/0EsnSugU+HZZrp/49XMyvdITyq3Q3QC/RDh2dIWD0VyXvz8
+       uDo6jvN9cx9rmej0sle/TXWYeLlNZrv5zQ8zLr/ZHWzOQAV45GdSgRREHKfHM9lj
+       i0qMagiTdk0df+/g78v8tQaefScj5JNbXqDive5HStdeogFMR7QkQ2VuZ2l6IEFs
+       YWV0dGlub2dsdSA8Y2VuZ2l6QGlzaS5lZHU+iQBLBBARAgALBQI2Q1PfBAsDAQIA
+       CgkQjZRGkY5cjCfDMgCgx8SYpbmMwCC3QoFaJdhBeHPtjCoAn3MZ75A0DmWlTjgI
+       akrLUaw3v5CGuQDNBDZDU+UQAwDUtvp8wrXXKqvhGMGBDLYYPWlgGhBAr2eoyS2r
+       n+JZPbDJp0KVygVfdkrWjqQpParzRRUHerhgGNnaiGZBB+XtDa70Ty8mKWGLyY3f
```

```
+       svtySSmVSDIjOCTIoMwhR+c3oBcAAgIC/2FVAllFaZWeuEpyjT5p4rOzgzpLSNTf
+       LV9Mav5hyuZJZYHlpibqt1uF5YiYGaE/ZafOP5pHvF89mOUZOy8Cj9rKc2AkoRWm
+       8XhDVL68MXjBUcMimNHkweOnn16iSNttm4kAPwMFGDZDU+WNlEaRjlyMJxECThwA
+       oOpfVLhHM1tqnq09SFptSoiEfxGQAKDFOb1pN8iuZslgttr7AcfAnImCYA==
+       =X+wc
+       -----END PGP PUBLIC KEY BLOCK-----
mnt-by: mnt-icann
source: ICANN

as-block:      AS0 - AS65535
descr:         as number space
country:       us
admin-c:       . . .
tech-c:        . . .
status:        UNALLOCATED
source:        ICANN
mnt-by:        mnt-icann
mnt-lower:     mnt-icann

inetnum:       0.0.0.0 - 255.255.255.255
netname:       Internet
descr:         ip number space
country:       us
admin-c:       . . .
tech-c:        . . .
status:        UNALLOCATED
source:        ICANN
mnt-by:        mnt-icann
mnt-lower:     mnt-icann
```

Here, we assume that ICANN runs its own repository. However this is not a requirement. Instead, it may publish its objects with one of the existing routing registries.

This set of seed objects needs to be signed with the hard coded ICANN key. Later, ICANN objects can be signed with the key in the ICANN key-cert object.

2 ICANN Assignments

Each time ICANN makes an assignment, it needs to create inetnum and as-block objects as appropriate and digitally sign them using the key in its key-cert object. For example:

```
as-block:     AS0 - AS500
```

```
descr:        arin's space
country:      us
status:       ALLOCATED
source:       icann
delegated:    arin
mnt-by:       mnt-icann

inetnum:      128.0.0.0 - 128.255.255.255
netname:      Internet portion
descr:        ip number space
country:      us
status:       ALLOCATED
source:       icann
delegated:    arin
mnt-by:       mnt-icann
```

3 Creating Routing Repositories

To enable a new routing repository, a repository object, a maintainer object and a key-cert object (if the maintainer object uses it) needs to be created and digitally signed by ICANN. For example:

```
  mntner:        mnt-ripe
  descr:         RIPE's maintainer
  auth:          <ripe's choice>
  mnt-by:        mnt-ripe
  referral-by:   mnt-icann
  admin-c:       . . .
  tech-c:        . . .
  upd-to:        . . .
  mnt-nfy:       . . .
  source:        RIPE

  key-cert: pgpkey-979979
  method: pgp
  owner:  . . .
  fingerpr: . . .
  certif: # this key is for illustration only
  +       -----BEGIN PGP PUBLIC KEY BLOCK-----
  +       Version: PGP for Personal Privacy 5.0
  +
  +       . . .
  +       -----END PGP PUBLIC KEY BLOCK-----
```

```
mnt-by: mnt-ripe
source: RIPE

repository:          RIPE
query-address:       whois.ripe.net 43
response-auth-type: rsa-pubkey some-incredibly-long-public-key
response-auth-type: none
remarks:             you can request rsa signature on queries
remarks:             PGP required on submissions
submit-address:      mailto://auto-dbm@ripe.net
submit-address:      rps-query://whois.ripe.net:43
submit-auth-type:    pgp-key crypt-pw mail-from
remarks:             these are the authentication types supported
mnt-by:              maint-ripe
expire:              0000 04:00:00
heartbeat-rate:      0000 01:00:00
...
remarks:             admin and technical contact, etc
source:              RIPE
```

This very first transaction of a new repository is placed in the new repository, not in the ICANN repository.

4 Security Consideration

This document describes ICANN procedures and initial RPSL seed objects. It does not define protocols or standards that need to be secured.

References

[1] C. Alaettinoglu, T. Bates, E. Gerich, D. Karrenberg, D. Meyer, M. Terpstra, and C. Villamizar: Routing Policy Specification Language (RPSL), RFC 2280.

[2] C. Villamizar, C. Alaettinoğlu, D. Meyer, S. Murphy, and C. Orange. Routing policy system security. Internet Draft draft-ietf-rps-auth-03, Network Information Center, April 1999.

[3] C. Villamizar, C. Alaettinoğlu, R. Govindan, D. Meyer. Distributed Routing Policy System. Internet Draft draft-ietf-rps-dist-01, Network Information Center, February 1999.

5 Authors' Addresses

Cengiz Alaettinoglu
USC Information Sciences Institute
email: cengiz@isi.edu

Curtis Villamizar
Avici Systems
email: curtis@avici.com

Ramesh Govindan
USC Information Sciences Institute
email: govindan@isi.edu