Internet Draft
Expires April 15, 2000
draft-ietf-rps-iana-02

Cengiz Alaettinoglu
USC/ISI
Curtis Villamizar
Avici Systems
Ramesh Govindan
USC/ISI
October 15, 1999

RPS IANA 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 IANA. This paper presents these seed objects and lists operations required from IANA.

1 Initial Seed

A public key of IANA 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. The following transaction (the transaction format is defined in [3]) contains these objects and is signed by this key:

```
mntner:        mnt-iana
descr:         iana's maintainer
admin-c:       JKR1
tech-c:        JKR1
upd-to:        JKRey@ISI.EDU
mnt-nfy:       JKRey@ISI.EDU
auth:          pgpkey-7F6AA1B9
mnt-by:        mnt-iana
referral-by:   mnt-iana
source:        IANA

key-cert: pgpkey-7F6AA1B9
method: pgp
owner:  iana-root (est. Nov 98) <iana@iana.org>
fingerpr: 71 09 2E 37 71 B8 0A 9C  3B 28 98 B4 F1 21 13 BB
certif: # this is the real IANA key
+ -----BEGIN PGP PUBLIC KEY BLOCK-----
+ Version: 2.6.2
+
+ mQCNAzZJ52sAAAEEAJ//C01YnlaGuXyrC16V7FphkRvBmcNU22TPOzrKnKjnWjH5
+ sJ5UQnGOpyhDc796gqBjY+lTLvPB9sFGJPWgxfNk2JQaxxLTD+tfqSsiURc/srpp
+ XohFAVR/fez8MOecISwvNpFh5VADuFuoNi7ZLuOwVTC4tM5RUONJa8l/aqG5AAUR
+ tCdpYW5hLXJvb3QgKGVzdC4gTm92IDk4KSA8aWFuYUBpYW5hLm9yZz4=
+ =sF4q
+ -----END PGP PUBLIC KEY BLOCK-----
mnt-by: mnt-iana
source: IANA

repository:         IANA
```

```
repository-cert:    PGPKEY-88BAC849
query-address:      http://www.iana.org
response-auth-type: none
submit-address:     http://www.iana.org
submit-auth-type:   none
expire:             0000 04:00:00
heartbeat-interval: 0000 01:00:00
admin-c:            JKR1
tech-c:             JKR1
mnt-by:             mnt-iana
source:             IANA

as-block:      AS0 - AS65535
descr:         as number space
country:       us
admin-c:       JKR1
tech-c:        JKR1
status:        UNALLOCATED
source:        IANA
mnt-by:        mnt-iana
mnt-lower:     mnt-iana

inetnum:       0.0.0.0 - 255.255.255.255
netname:       Internet
descr:         ip number space
country:       us
admin-c:       JKR1
tech-c:        JKR1
status:        UNALLOCATED
source:        IANA
mnt-by:        mnt-iana
mnt-lower:     mnt-iana

timestamp: 19991001 01:00:00 +00:00

signature:
+ -----BEGIN PGP SIGNATURE-----
+ Version: 2.6.2
+
+ iQCVAwUBOAd3YENJa8l/aqG5AQFVdAP9Ho2TSLGXiDi6v1McsKY4obO32EtP44Jv
+ tpNWiRRz47WIpMBmzUrQajBDNNXzwq9r9mGC75Pg0MMwTDfvA47o6mnIGdT9XyZz
+ s9HlDGOqhklIjHOxXFDrBiz3u7eWEf3vmDCXt6UYg9lUtRKefkWtR5wD1Q1zDMSc
+ 7Ya7PE6X8SU=
+ =sAft
+ -----END PGP SIGNATURE-----
```

The above text has no extra white space characters at the end of each line, and contains no tab characters. All blank line sequences contain only a single blank line.

In this case, we assumed that IANA runs its own repository. However this is not a requirement. Instead, it may publish this transaction with an existing routing registry.

2 IANA Assignments

Each time IANA 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:       iana
delegated:    arin
mnt-by:       mnt-iana

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

3 Creating Routing Repositories

To enable a new routing repository, a repository object, a maintainer object and a key-cert object need to be created and digitally signed by IANA. For example:

```
  mntner:         mnt-ripe
  descr:          RIPE's maintainer
  auth:           <ripe's choice>
  mnt-by:         mnt-ripe
  referral-by:    mnt-iana
  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://whois.ripe.net
response-auth-type: PGPKEY-23F5CE35 # pointer to key-cert object
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-db
expire:             0000 04:00:00
heartbeat-interval: 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 IANA repository.

4 Security Considerations

Routing policy system security document [2] defines an hierarchical authorization model for objects stored in the routing registries. This document specifies the seed objects and the actions need to be taken by IANA to maintain the root of that authorization hierarchy.

5 IANA Considerations

This whole document is for detailed consideration by IANA.

References

[1] C. Alaettinoglu, T. Bates, E. Gerich, D. Karrenberg, D. Meyer, M. Terpstra, and C. Villamizar: Routing Policy Specification Language (RPSL), RFC 2622.

[2] C. Villamizar, C. Alaettinoğlu, D. Meyer, S. Murphy, and C. Orange. Routing policy system security. Internet Draft draft-ietf-rps-auth-04, Network Information Center, April 1999.

[3] C. Villamizar, C. Alaettinoğlu, R. Govindan, D. Meyer. Distributed Routing Policy System. Internet Draft draft-ietf-rps-dist-02, Network Information Center, February 1999.

6 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

Full Copyright Statement

Notices