

Network Working Group
Request for Comments: 2754
Category: Informational

C. Alaettinoglu
USC/ISI
C. Villamizar
Avici Systems
R. Govindan
USC/ISI
January 2000

RPS IANA Issues

Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2000). All Rights Reserved.

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.

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.

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
+
+ mQCNAzZJ52sAAAEAAJ//C01YnlaGuXyrC16V7FphkRvBmcNU22TPOzrKnKjnWjH5
+ sJ5UQnGOPYhDc796gqBjY+lTLvPB9sFGJPWgxfNk2JQaxxLTD+tfqSsiURc/srpp
+ XohFAVR/fez8MOecISwvNpFh5VADuFuoNi7ZLuOwVTC4tm5RU0NJa8l/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. The page break in the text is also 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] Alaettinoglu, C., Bates, T., Gerich, E., Karrenberg, D., Meyer, D., Terpstra, M. and C. Villamizar, "Routing Policy Specification Language (RPSL)", RFC 2622, June 1999.
- [2] Villamizar, C., Alaettinoglu, C., Meyer, D., Murphy, S. and C. Orange, "Routing Policy System Security", RFC 2725, December 1999.
- [3] Villamizar, C., Alaettinoglu, C., Govindan, R. and D. Meyer, "Distributed Routing Policy System", Work in Progress.

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

7 Notices

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

8 Full Copyright Statement

Copyright (C) The Internet Society (2000). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.

