How to debug RPKI issues? Data structures & tools

NANOG 85

Job Snijders
Fastly / OpenBSD
job@fastly.com / job@openbsd.org


FREE TENDO

Agenda

- What is a RPKI Signed Object?
- Quick overview of object types: Certs, ROAs, CRLs, Manifests
- Exploring RPKI from root (Trust Anchor) to its edges (ROAs)
- Exploring RPKI from edge back to the top
- Transitive timers & revocation lists
- Questions?

What is a RPKI Signed Object? Easy! :-) :-) :-)

```
feather$ cd /var/cache/rpki-client/chloe.sobornost.net/rpki/RIPE-nljobsnijders/
feather$ ls
1m9l-LVo9u9IU3YCHXQBJWyIfdo.roa     8EjgZ6BLB_EFHp9nPxEgX5icjjM.roa     OOFPkv3HzPv8GCNhUjrifWl-lS8.mft     ZKleK6jOSHKLwPONR0e5XVcwqAM.roa
voibVdC3Nzl9dcSfSFuFj6mK0R8.cer
5GzpWH5N-vMm_nh7A93VwzaW4zk.gbr     OOFPkv3HzPv8GCNhUjrifWl-lS8.crl     XUJQ4tgdREjYop786R0p_wdeyeI.cer     rZWj66_V88W5B41mgMEm-TNr_EU.roa
feather$ cat 1m9l-LVo9u9IU3YCHXQBJWyIfdo.roa
0??0??1 *?H??
        `?He0-
        ?0%?000?H??
        *?H??  0        -?????0??0??0
?0?     *?H??03110/U(D66F65F8B568F6EF485376021D7401256C887DDA0?"0
??\Y??.???E???????????x?%k????CF???B??kH
I????a?t?
b+.????yf}???H;?}??v???Ã
8??^????`Z?B???X??n_?6?k?N_?h?(?
??1X>v_???8??N??Q?B?-d?n?s?]J??}??#?]???:??<?dFjX??????A??X???^x?F8????DV????C?X?4?1????w3??0?0U?oe?h??HSvt%l?}?0U#0?8?O??????#aR:?}i~?/0U ?0
                                                                                                                                                0
+0dU]0[0Y?W?U?Srsync://chloe.sobornost.net/rpki/RIPE-nljobsnijders/OOFPkv3HzPv8GCNhUjrifWl-lS8.crl0+X0V0+0?Hrsync://rpki.ripe.net/repository/DEFAULT/
OOFPkv3HzPv8GCNhUjrifWl-lS8.cer0U??0?+
     ??0??0+0
?)https://chloe.sobornost.net/rpki/news.xml+?00/RIPE-nljobsnijders/1m9l-LVo9u9IU3YCHXQBJWyIfdo.roa0+0
        *?H??                                0-??0
?/?
   .?7  ?R?0?-?;?l:W?  ?:?{6R,?????,?x????g????pV?i??l????f???s?A?7??m&J??§1?????bH???
                                                                                ?]?i<T?&;       <{h)=&???at?ZB`?`1,I??G???????a:h???LQ?OsX
                                                                                                                                ?v??ub??h????G????
                                                                                                                                                :P?{X?????
j?f??(?/C?r?{?J
     <?O??}c2-\2??"+????l??7?9?9B???$????1??0????oe?h??HSvt%l?}?0
        1                                                       `?He?k0 *?H??
?       *?H???\?v?1??G$???p????]???]??0
?7E?d@??uR?rX?.??Q!?m~?~???????d1zN?n??V?5??+??j?
0?]?    "\      Ia@                          ??v\e?`??t?-1???!?????`??P?|F??r?[AX??{?R??'?*????!?#KI%???#&???.OF??+???J,?   VH??"Ha&_?d?zs?)??/?vO??m?p? m?A?
                  \???|??X9?I??~?M)?W*P??1?3
                                     K???B
feather$
```

Demystifying Signed Objects – what are they really

- Binary blobs encoded following a serialization format for ASN.1
- Each blob is identifiable by its hash (non-malleable)
- Each Signed Object is structured according to Cryptographic Message Syntax (CMS).
- Think of CMS as an *envelope:* on the outside of the envelope contains a signature which covers what's inside.

Demystifying Signed Objects – what are they #2

What's inside the envelope?

- **The eContent:**
  - In the case of a ROA: Origin AS + list of prefixes that ASN can originate
- **The X.509 EE certificate:**
  - AKI, AIA, SKI, CRLDP, CP, SIA, ipAddrBlocks
  - A hash
  - A signature

Discovering objects: going from “Root” to “Edge”

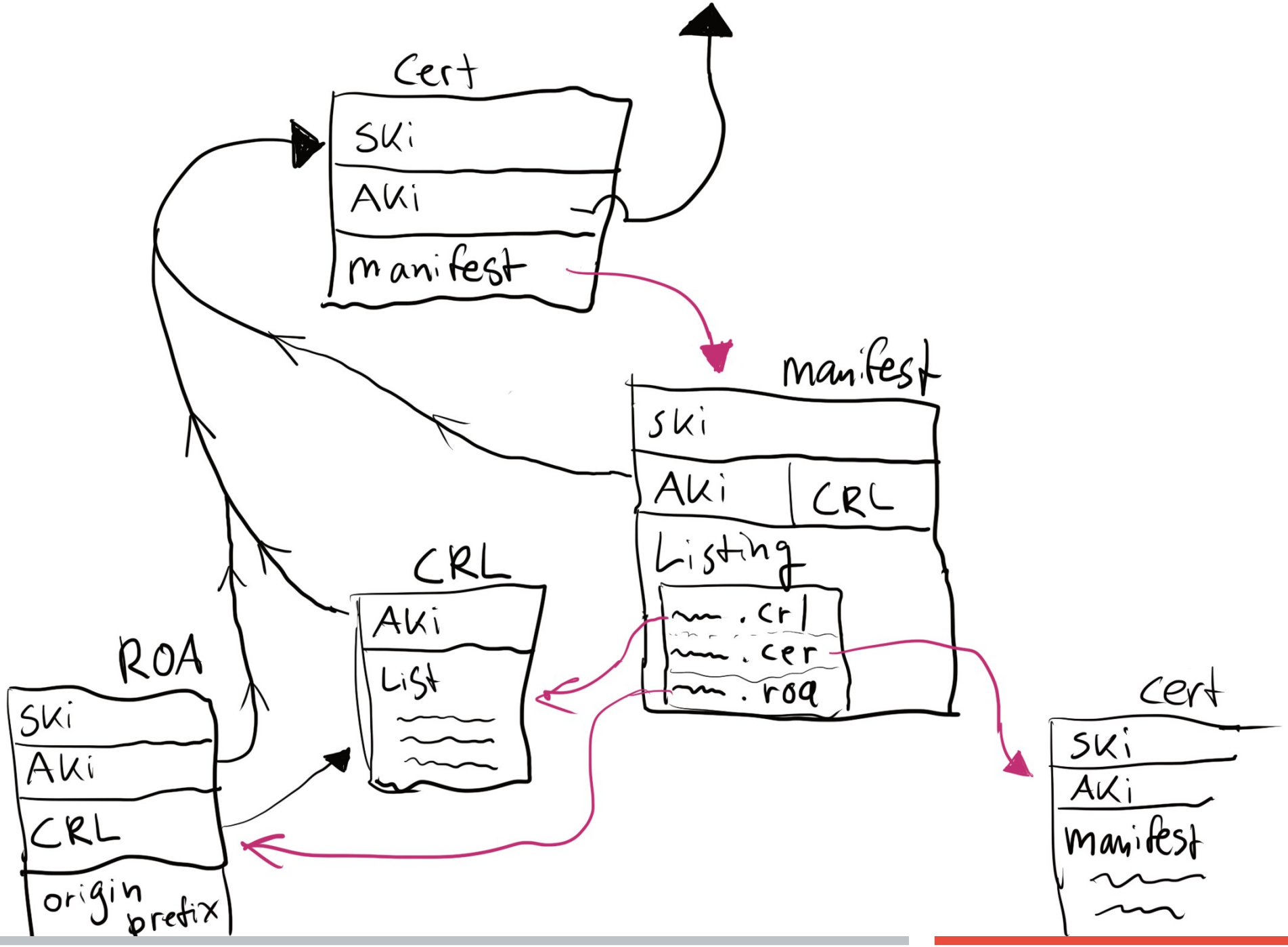
Visualize the RPKI is a graph shaped as a pyramid:

- The “root” is a Trust Anchor (assumed trust)
- There are intermediate nodes (Certificate Authorities)
- The edges are things like ROAs, GBRs, CRLs (derived trust)

From Root to Edge:

- Download TAL
- Download Trust Anchor (self-signed X.509 certificate)
- Follow SIA to top-level manifest
- Download Manifest
- Open Manifest for listing of files (each Manifest contains a CRL)
- Download each individual file
- If a file is a X.509 certificate → follow its SIA to its manifest

And so on...


Cert
SKi
AKi
manifest
manifest
ski
AKi
CRL
Listing
.crl
.cer
.roa
CRL
AKi
List
ROA
SKi
AKi
CRL
origin prefix
cert
SKi
AKi
manifest

The other way around: from Edge to Root

Each Signed Object contains pointers to its parent: AIA & AKI

AIA = Authority Information Access

AKI = Authority Identifier Key

Each signature inside a Signed Object can be verified with the public key of its parent (the Authority): a chain of signatures leading all the way up to the root (Trust Anchor).

From the same project that brought you OpenSSH, LibreSSL, and OpenBGPD: OpenBSD delivers again!

rpki-client

Getting started: install & run rpki-client

```
root@debian-unstable# apt install -y rpki-client

… MACHINE GO BRRR …

root@debian-unstable# systemctl start rpki-client

… MACHINE GO BRRR …

root@debian-unstable# cd /var/cache/rpki-client/

root@debian-unstable:/var/cache/rpki-client# ls
0.sb/                  r.magellan.ipxo.com/     rpki-rsync.e15f.net/     rpki.arin.net/
rpki.owl.net/          rpki.xindi.eu/           rsync.krill.cloud/       ca.rg.net/
repo1.rpki.qs.nu/      rpki.admin.freerangecloud.com/                    rpki.august.tw/
rpki.ripe.net/         rpki1.rpki-test.sit.fraunhofer.de/                ta/
chloe.sobornost.net/   repository.lacnic.net/   rpki.afrinic.net/
rpki.caramelfox.net/   rpki.roa.net/           rpki1.terratransit.de/
nostromo.heficed.net/  rpki-repo.as207960.net/  rpki.apnic.net/
rpki.multacom.com/     rpki.sub.apnic.net/      rpkica.mckay.com/
```

rpki-client is the “*tcpdump*” of the RPKI

What is a Manifest?

```
feather$ rpki-client -f OOFPkv3HzPv8GCNhUjrifWl-lS8.mft
File: OOFPkv3HzPv8GCNhUjrifWl-lS8.mft
Hash identifier: VTfnlTAHEqpNfL2hyoVoNEKYYtv048SbIy9b91Nq8nc=
Subject key identifier: 6B:F9:B9:95:64:CA:55:F7:23:48:BF:63:6B:0B:55:41:D5:66:9F:F7
Authority key identifier: 38:E1:4F:92:FD:C7:CC:FB:FC:18:23:61:52:3A:E2:7D:69:7E:95:2F
Certificate serial: 7362
Authority info access: rsync://rpki.ripe.net/repository/DEFAULT/OOFPkv3HzPv8GCNhUjrifWl-lS8.cer
Manifest Number: 6F69
Manifest valid since: Apr 25 18:51:16 2022 GMT
Manifest valid until: Apr 26 00:51:16 2022 GMT
    1: 1m9l-LVo9u9IU3YCHXQBJWyIfdo.roa
         hash kaQlVIUVe24w3PciEVPJMQYqU0IQuQ5QISd8G2YaKyg=
    2: 5GzpWH5N-vMm_nh7A93VwzaW4zk.gbr
         hash tPLdPQGS+JZ7zsGEDPyyML8tzxgTi0VAPTlvNGrrJUY=
    3: 8EjgZ6BLB_EFHp9nPxEgX5icjjM.roa
         hash SOEcjkVgU5iVKTy6DA/on2jX0uBNJYLk92JjWdMtfpk=
    4: OOFPkv3HzPv8GCNhUjrifWl-lS8.crl
         hash AkzoToGsNMsoXkPQ+RhMiDIbPltVdA8PryYNyAXvLXQ=
    5: XUJQ4tgdREjYop786R0p_wdeyeI.cer
         hash sMTKa0xoD1jau2fF84qEfmtWgp/aXkLz+nKDb0ya/38=
    6: ZKleK6jOSHKLwPONR0e5XVcwqAM.roa
         hash /yl2/U6f80H7GQhsHX8uoNQbMDUr22unPB/T+9vWkiY=
    7: rZWj66_V88W5B41mgMEm-Tnr_EU.roa
         hash SYWMTnEkWN5L+qD/TgYvMakQ1rSktXsgJrR1dLu8GTA=
    8: voibVdC3Nzl9dcSfSFuFj6mK0R8.cer
         hash zoHLGdLDyxA2/z8yMXVxHkjFqJZlD9BsI5Qv1NedWkE=
Validation: OK
```

What do Manifests do?

- Detect replay attacks
- Detect unauthorized in-flight modification of signed objects
- Detect unauthorized in-flight deletion of signed objects
- Essential mechanism to robustly bundle ROAs together

What is a CRL?

```
feather$ rpki-client -f OOFPkv3HzPv8GCNhUjrifWl-lS8.crl | head -n 12
File: OOFPkv3HzPv8GCNhUjrifWl-lS8.crl
Hash identifier: MaoadTJFQRqgidyhg75B7sBzc/OZ3q0BJLMLGwARHME=
Authority key identifier: 38:E1:4F:92:FD:C7:CC:FB:FC:18:23:61:52:3A:E2:7D:69:7E:95:2F
CRL Serial Number: 6F69
CRL valid since: Apr 25 18:51:16 2022 GMT
CRL valid until: Apr 26 00:51:16 2022 GMT
Revoked Certificates:
    Serial:       05   Revocation Date: Sep 27 15:51:34 2021 GMT
    Serial:     0455   Revocation Date: Sep 27 15:51:34 2021 GMT
    Serial:     0D23   Revocation Date: May 04 14:55:45 2021 GMT
    Serial:     18F6   Revocation Date: Jul 06 13:03:23 2021 GMT
    Serial:     18F7   Revocation Date: Jul 06 13:03:28 2021 GMT
    Serial:     18F8   Revocation Date: Jul 06 13:03:22 2021 GMT
```

What is a GBR?

```
feather$ rpki-client -f 5GzpWH5N-vMm_nh7A93VwzaW4zk.gbr
File: 5GzpWH5N-vMm_nh7A93VwzaW4zk.gbr
Hash identifier: tPLdPQGS+JZ7zsGEDPyyML8tzxgTi0VAPTlvNGrrJUY=
Subject key identifier: E4:6C:E9:58:7E:4D:FA:F3:26:FE:78:7B:03:DD:D5:C3:36:96:E3:39
Certificate serial: 07
Authority key identifier: 38:E1:4F:92:FD:C7:CC:FB:FC:18:23:61:52:3A:E2:7D:69:7E:95:2F
Authority info access: rsync://rpki.ripe.net/repository/DEFAULT/OOFPkv3HzPv8GCNhUjrifWl-
lS8.cer
vcard:
BEGIN:VCARD
VERSION:4.0
FN:Job Snijders
ORG:Job Snijders
ADR;TYPE=HOME:;;Theodorus Majofskistraat 100;Amsterdam;;1065 SZ;The Netherlands
TEL;TYPE=VOICE,TEXT,HOME;VALUE=uri:tel:+31-6-54942365
EMAIL:job@sobornost.net
END:VCARD
Validation: OK
```

What is a ROA?

```
feather$ rpki-client -f ZKleK6jOSHKLwPONR0e5XVcwqAM.roa
File: ZKleK6jOSHKLwPONR0e5XVcwqAM.roa
Hash identifier: /yl2/U6f80H7GQhsHX8uoNQbMDUr22unPB/T+9vWkiY=
Subject key identifier: 64:A9:5E:2B:A8:CE:48:72:8B:C0:F3:8D:47:47:B9:5D:57:30:A8:03
Certificate serial: 2D0F
Authority key identifier: 38:E1:4F:92:FD:C7:CC:FB:FC:18:23:61:52:3A:E2:7D:69:7E:95:2F
Authority info access: rsync://rpki.ripe.net/repository/DEFAULT/OOFPkv3GCNhUjrifWl-lS8.cer
ROA valid until: Jul 01 00:00:00 2022 GMT
asID: 15562
    1: 2a0e:b240:3::/48 maxlen: 48
Validation: OK
```

What is a BGPsec Router key?

```
feather$ rpki-client -f XUJQ4tgdREjYop786R0p_wdeyeI.cer
File: XUJQ4tgdREjYop786R0p_wdeyeI.cer
Hash identifier: sMTKa0xoD1jau2fF84qEfmtWgp/aXkLz+nKDb0ya/38=
Subject key identifier: 5D:42:50:E2:D8:1D:44:48:D8:A2:9E:FC:E9:1D:29:FF:07:5E:C9:E2
Authority key identifier: 38:E1:4F:92:FD:C7:CC:FB:FC:18:23:61:52:3A:E2:7D:69:7E:95:2F
Certificate serial: 34B5
Authority info access: rsync://rpki.ripe.net/repository/DEFAULT/OOFPkv3HzNhUjrifWl-lS8.cer
BGPsec P-256 ECDSA public key:
MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEgFcjQ/g//LAQerAH2Mpp+GucoDAGBbhIqD33wNPsXxnAGb+mtZ7XQr
VO9DQ6UlAShtig5+QfEKpTtFgiqfiAFQ==
Valid until: 2022-11-09T17:04:39Z
Subordinate Resources:
    1: AS: 15562
Validation: OK
```

Timers and Revocation Lists

There are a few ways objects might be considered *invalid:*

- The certificate's serial is listed on the CRL
- The certificate has expired
- The manifest has expired
- The CRL has expired
- Adjacent Signed Objects (listed on the Manifest) are missing

References

Full data dump (JSON encoded) of RPKI:

https://console.rpki-client.org/dump.json

The rpki-client utility: https://www.rpki-client.org

Part of OpenBSD, also available in Debian, EPEL, etc

Questions?

Feel free to email me any questions about RPKI and BGP!

job@fastly.com