Can ROAs Replace LOAs? Research into Route Validation and RPKI as an alternative to Letters of Authority

Aftab Siddiqui | Christopher Hawker

siddiqui@isoc.org | chris@thesysadmin.au

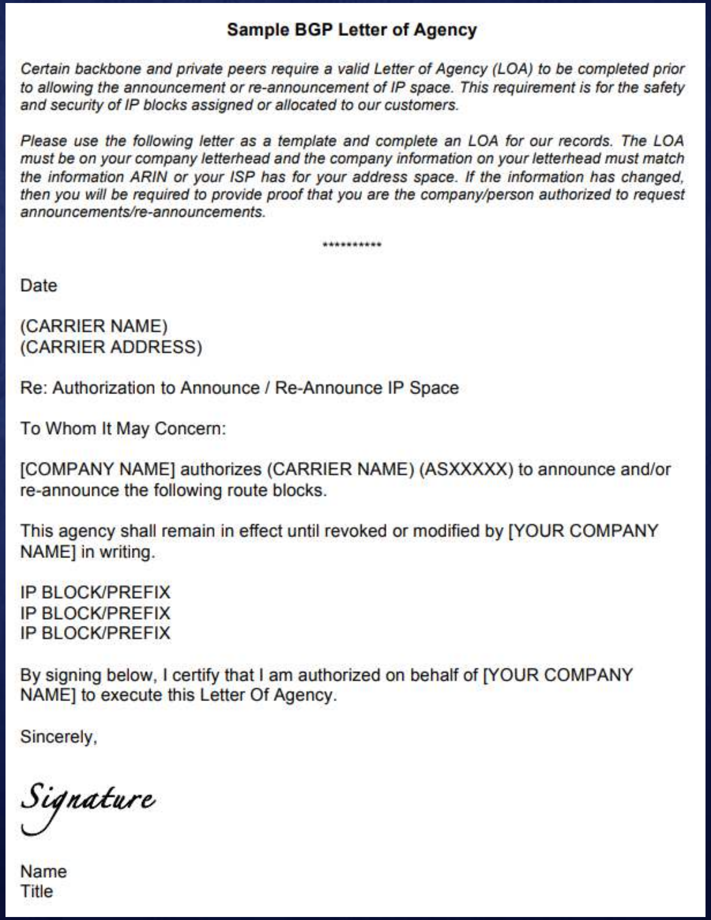
APNIC 57 Routing Security SIG Meeting

Thursday, 29 February 2024

2024 APRICOT
APNIC 57
BANGKOK, THAILAND
21 February – 1 March 2024
#apricot2024

Introduction – What are LOAs?

- A document used to demonstrate authority to (re)announce IP resources.
- Used for at least the last 2 decades since the days when network operators personally knew one another and there was an inherent level of trust.



Sample BGP Letter of Agency

Certain backbone and private peers require a valid Letter of Agency (LOA) to be completed prior to allowing the announcement or re-announcement of IP space. This requirement is for the safety and security of IP blocks assigned or allocated to our customers.

Please use the following letter as a template and complete an LOA for our records. The LOA must be on your company letterhead and the company information on your letterhead must match the information ARIN or your ISP has for your address space. If the information has changed, then you will be required to provide proof that you are the company/person authorized to request announcements/re-announcements.

****

Date

(CARRIER NAME)
(CARRIER ADDRESS)

Re: Authorization to Announce / Re-Announce IP Space

To Whom It May Concern:

[COMPANY NAME] authorizes (CARRIER NAME) (ASXXXXX) to announce and/or re-announce the following route blocks.

This agency shall remain in effect until revoked or modified by [YOUR COMPANY NAME] in writing.

IP BLOCK/PREFIX
IP BLOCK/PREFIX
IP BLOCK/PREFIX

By signing below, I certify that I am authorized on behalf of [YOUR COMPANY NAME] to execute this Letter Of Agency.

Sincerely,

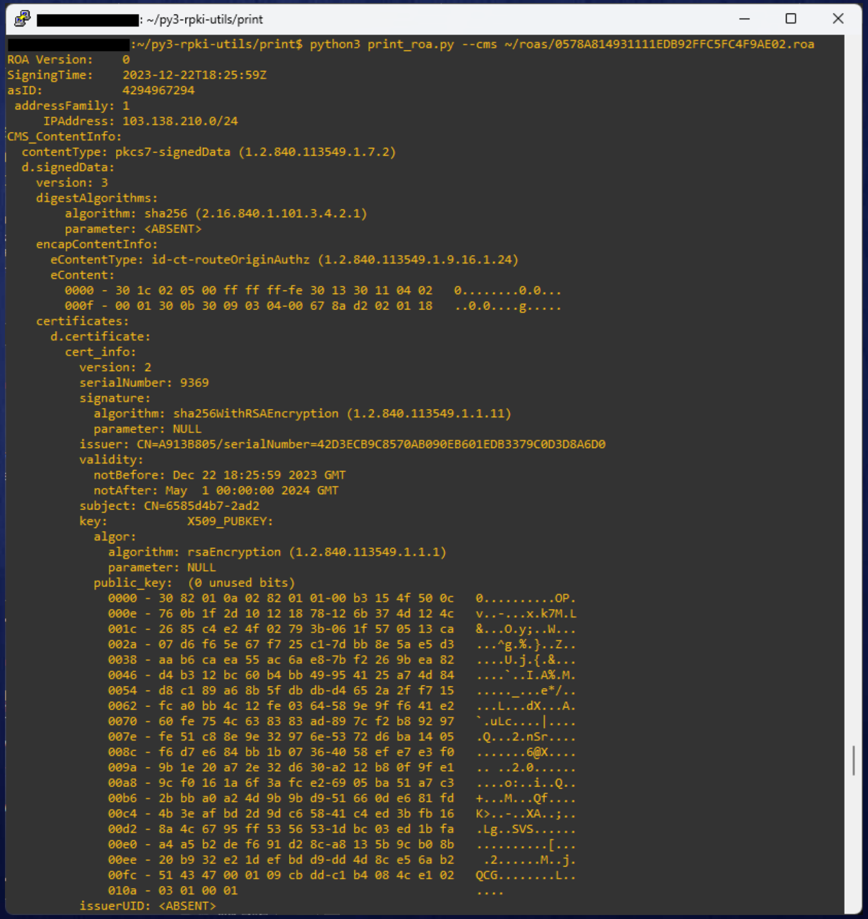
Signature

Name
Title

Figure – An example Letter of Authority. Source: https://www.academia.edu/13161976/Sample_BGP_Letter_of_Agency

Introduction – What are ROAs?

- Cryptographically-signed objects under RPKI which allow networks to determine what AS numbers are permitted to announce what prefixes.
- A benefit of using ROAs is that network operators can automate prefix filtering using Route Object Validation with BGP prefix filtering mechanisms.



[redacted]: ~/py3-rpki-utils/print

```
[redacted]:~/py3-rpki-utils/print$ python3 print_roa.py --cms ~/roas/0578A814931111EDB92FFC5FC4F9AE02.roa
ROA Version:    0
SigningTime:    2023-12-22T18:25:59Z
asID:           4294967294
 addressFamily: 1
     IPAddress: 103.138.210.0/24
CMS_ContentInfo:
  contentType: pkcs7-signedData (1.2.840.113549.1.7.2)
  d.signedData:
    version: 3
    digestAlgorithms:
        algorithm: sha256 (2.16.840.1.101.3.4.2.1)
        parameter: <ABSENT>
    encapContentInfo:
      eContentType: id-ct-routeOriginAuthz (1.2.840.113549.1.9.16.1.24)
      eContent:
        0000 - 30 1c 02 05 00 ff ff ff-fe 30 13 30 11 04 02   0........0.0...
        000f - 00 01 30 0b 30 09 03 04-00 67 8a d2 02 01 18   ..0.0....g.....
    certificates:
      d.certificate:
        cert_info:
          version: 2
          serialNumber: 9369
          signature:
            algorithm: sha256WithRSAEncryption (1.2.840.113549.1.1.11)
            parameter: NULL
          issuer: CN=A913B805/serialNumber=42D3ECB9C8570AB090EB601EDB3379C0D3D8A6D0
          validity:
            notBefore: Dec 22 18:25:59 2023 GMT
            notAfter: May  1 00:00:00 2024 GMT
          subject: CN=6585d4b7-2ad2
          key:           X509_PUBKEY:
            algor:
              algorithm: rsaEncryption (1.2.840.113549.1.1.1)
              parameter: NULL
            public_key:  (0 unused bits)
              0000 - 30 82 01 0a 02 82 01 01-00 b3 15 4f 50 0c   0..........OP.
              000e - 76 0b 1f 2d 10 12 18 78-12 6b 37 4d 12 4c   v..-...x.k7M.L
              001c - 26 85 c4 e2 4f 02 79 3b-06 1f 57 05 13 ca   &...O.y;..W...
              002a - 07 d6 f6 5e 67 f7 25 c1-7d bb 8e 5a e5 d3   ...^g.%.}..Z..
              0038 - aa b6 ca ea 55 ac 6a e8-7b f2 26 9b ea 82   ....U.j.{.&...
              0046 - d4 b3 12 bc 60 b4 bb 49-95 41 25 a7 4d 84   ....`..I.A%.M.
              0054 - d8 c1 89 a6 8b 5f db db-d4 65 2a 2f f7 15   ....._...e*/..
              0062 - fc a0 bb 4c 12 fe 03 64-58 9e 9f f6 41 e2   ...L...dX...A.
              0070 - 60 fe 75 4c 63 83 83 ad-89 7c f2 b8 92 97   `.uLc....|....
              007e - fe 51 c8 8e 9e 32 97 6e-53 72 d6 ba 14 05   .Q...2.nSr....
              008c - f6 d7 e6 84 bb 1b 07 36-40 58 ef e7 e3 f0   .......6@X....
              009a - 9b 1e 20 a7 2e 32 d6 30-a2 12 b8 0f 9f e1   .. ..2.0......
              00a8 - 9c f0 16 1a 6f 3a fc e2-69 05 ba 51 a7 c3   ....o:..i..Q..
              00b6 - 2b bb a0 a2 4d 9b 9b d9-51 66 0d e6 81 fd   +...M...Qf....
              00c4 - 4b 3e af bd 2d 9d c6 58-41 c4 ed 3b fb 16   K>..-..XA..;..
              00d2 - 8a 4c 67 95 ff 53 56 53-1d bc 03 ed 1b fa   .Lg..SVS......
              00e0 - a4 a5 b2 de f6 91 d2 8c-a8 13 5b 9c b0 8b   ..........[...
              00ee - 20 b9 32 e2 1d ef bd d9-dd 4d 8c e5 6a b2    .2......M..j.
              00fc - 51 43 47 00 01 09 cb dd-c1 b4 08 4c e1 02   QCG........L..
              010a - 03 01 00 01                                 ....
          issuerUID: <ABSENT>
```

Figure – The Route Origin Authorisation certificate for 103.138.210.0/24 generated using ISOC-Research's Python 3 Utilities for RPKI (https://github.com/ISOC-Research/py3-rpki-utils).

The Problem...

Why are we looking into this?

The Problem with LOAs…

- Reliance on confidence-based acceptance of information on LOA.
- Extremely easy to falsify (can be done in as little as 10 mins).
- Requires additional work to verify contents (no method to automate validation).
- Needs to be manually revoked through a follow-up letter when authority is withdrawn.

Real-World Example of a #FakeLOA

- IIJ received a /16 IPv4 prefix on 21 Oct 2014.
- On 05 Jan 2015 “ISP X” began to announce IIJ’s /16 as 2 x /17 routes without authorization.
- JANOG’s mailing list received a post about these announcements on 04 Feb 2015.
- IIJ contacted ISP X to withdraw the routes on 04 Feb 2015 and again on 06 Feb 2015.
- Routes were finally withdrawn on 07 Feb 2015.

#FakeLOA Investigation

- ISP X received an LOA from their customer for the prefixes.
- IIJ never authorized the announcements.
- The company on the LOA was a family company of the former holder.
- Email address on LOA was incorrect (newly registered domain name in 2014) and phone number was wrong.
- Contact with the former resource holder confirmed the domain name was not theirs, that they did not sign the LOA nor was their company aware…
- If it looks like a fake and smells like a fake, it is a #FakeLOA!

The Survey…

The collection of the information, compilation of data and analysis.

The Survey

- Aftab and I reached out to several NOGs over a 2-month period (mid-November 2023 to mid-January 2024) and conducted a survey.
- We surveyed individuals representing 61 unique networks.
- The 61 networks utilised 51 different upstream providers.
- Some respondents did not answer all questions, and this has been factored into statistics where relevant.

Requirement to provide LOA

[Note: Respondents were permitted to select multiple options.]

- 28 respondents provided LOAs to confirm ownership/authorisation.
- 10 stated that it was to validate downstream resources.
- 8 stated it was to comply with regulatory requirements and industry standards.
- 5 were for other reasons.

Required LOA Format

- 24 upstreams requested an LOA on an official letterhead, in PDF format, sent to them as an email attachment.
- 6 required an email from a corporate email address.
- 1 accepted an email saved as a PDF from the resource holder as authorisation a respondent was permitted to announce their resources.
- 1 (most interestingly) accepted a plain-text file that “was typed up in Notepad”.

Understanding of LOAs

For LOAs to be effective, it requires an understanding about how they are used and what they must contain.

- 42 respondents had a clear understanding,
- 3 had a moderately clear understanding,
- 3 either had a somewhat clear, neither clear or unclear or completely unclear understanding, and
- 13 did not answer.

Security of Data within LOAs

Network operators need to be reassured that their information contained within the LOA is only used for the intended purpose – to demonstrate authority for the announcement of prefixes.

- 30 were very comfortable,
- 5 were somewhat comfortable,
- 6 were moderately comfortable,
- 7 were not comfortable at all, and
- 13 did not respond.

Challenges with using LOAs

- 36 respondents encountered no challenges,
- 11 did and had concerns, and
- 14 did not answer the question.

Some of the concerns were:

- That ISPs still requested an alternate method of authorisation, regardless of the provision of an LOA.
- LOAs can be falsified relatively easily and quickly.
- Networks are unable to provide upstreams with prefixes being advertised by their downstream peers due to those downstreams not providing LOAs.
- Delays with addition of authorised routes to route filters and subsequent withdrawal of prefixes.

Are LOAs really necessary?

- 11 believe that a request from an upstream for an LOA is extremely essential in ensuring the security and reliability of their service,
- 9 believe LOAs are moderately essential,
- 15 believe that LOAs are somewhat essential,
- 13 believe that they are not necessary, and
- 13 did not answer the question.

Are there risks with providing LOAs?

- 29 respondents were not aware of any potential risks when providing LOAs to an upstream peer,
- 19 respondents were, and
- 13 did not answer.

- Lack of Revocation Date can cause issues with having prefixes blocked/filtered.
- LOAs do not demonstrate whether a prefix has been delegated by an RIR/NIR.
- It can take time for advertisements to be filtered/blocked when authority is revoked whereas ROAs can be revoked with minimal interaction within hours.

What exactly is RPKI?

Martin Levy, in a Cloudflare Blog article titled "RPKI – The required cryptographic upgrade to BGP routing" (https://blog.cloudflare.com/rpki) defines it in one sentence as "a cryptographic method of signing records that associate a BGP route announcement with the correct originating AS number".

Respondents were asked about the definition of RPKI, and:

- 41 said that RPKI associates prefixes with an origin ASNs using digital certificates,
- 3 said that it secures data transmission over the internet preventing unauthorised access to traffic, and
- 17 did not answer the question.

Familiarity with implementation and usage of ROAs

- 31 respondents were very familiar with how to implement and use ROAs,
- 6 were moderately familiar,
- 4 were somewhat familiar,
- 1 was not so familiar, and
- 2 were not familiar at all.
- 17 did not answer the question.

APNIC has an excellent Help Centre article for its members (https://help.apnic.net/s/article/roa-objects) that details step-by-step how to enable Resource Certification and create ROA objects.

The question…

Can ROAs be used as a replacement for LOAs?

Can ROAs replace LOAs?

- 29 respondents said yes,
- 3 said that they cannot,
- 10 believe they can with additional verification steps, and
- 6 were not sure.

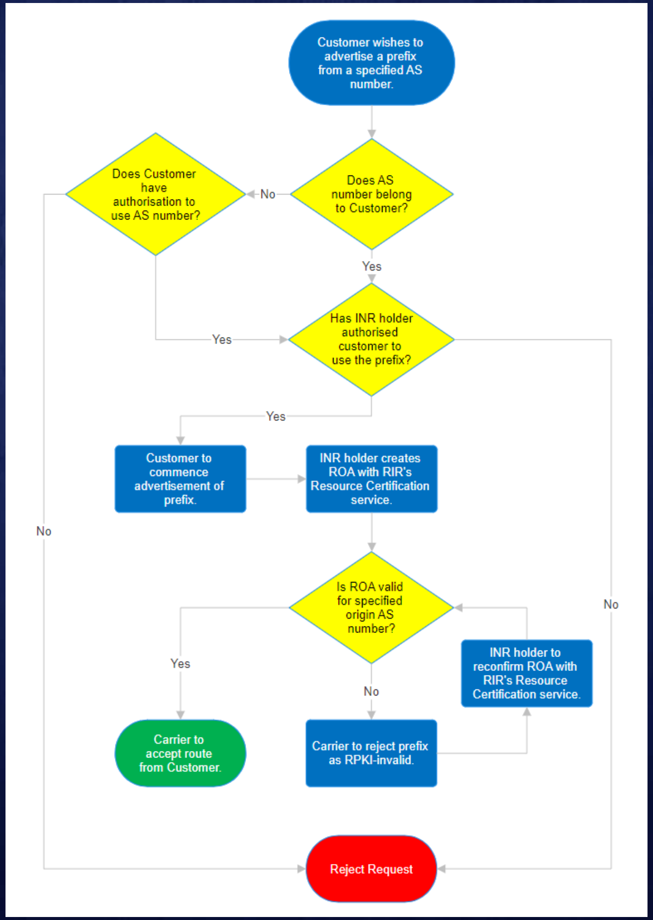

Customer wishes to advertise a prefix from a specified AS number.
Does AS number belong to Customer?
No
Does Customer have authorisation to use AS number?
Yes
Yes
Has INR holder authorised customer to use the prefix?
Yes
Customer to commence advertisement of prefix.
INR holder creates ROA with RIR's Resource Certification service.
No
Is ROA valid for specified origin AS number?
No
Yes
No
INR holder to reconfirm ROA with RIR's Resource Certification service.
Carrier to accept route from Customer.
Carrier to reject prefix as RPKI-invalid.
Reject Request

Figure – Flow Chart for utilization of ROAs as authority to advertise INRs.

Can ROAs be used for legal verification?

- 25 agreed that ROAs can be used for legal verification to confirm a given origin AS can route a prefix,
- 3 do not believe they can be,
- 10 agree they could be with additional verification methods,
- 6 were not sure if they could be or not, and
- 17 respondents did not answer the question.

The 'I' in RPKI Does Not Stand for Identity

- RFC 9255 specifies that RPKI does not associate Internet Number Resources (INRs) to INR holders.
- ROAs MUST NOT be used to authenticate real-world documents or transactions.
- The purpose of ROAs is to validate the origin AS of an INR.

- Using ROAs is not designed to authenticate an entity. Entity verification is external to this process.
- ROAs do exactly what an LOA does - authorize an origin AS to announce a specified prefix.

Additional Comments

- Newer networks that formed post-exhaustion and lease IP space from [Transit Provider] won't be able to have ROAs created for these prefixes due to them not being an [RIR] member and not having access to [RIR]'s RPKI infrastructure.
- Autonomous System Provider Authorization (ASPA) would probably also be needed to completely replace LOAs.
- If an ROA exists for a given prefix, it suggests that a validated resource holder has given consent for the use of the prefix by the specified ASN.
- Overall, I believe that this would cut down on errors, route hijacks and implementation time.

Thankyou!