

# how to detect alignment of RPKI certificates and registry (sub)accounts

Summary: the pipeline in one go

```
# for some repository..  
rsync --delete -az rpki.cnnic.cn::rpki cnnic  
# for some certificate e.g. Y1vTOT_M9475iEK4qDNi1UnlneM.cer  
./readwhichopenssl.py ./cnnic/A9162E3D0000/Y1vTOT_M9475iEK4qDNi1UnlneM.ce | \  
./delegfilter.py -s, -t cc,orgid -n 3 | \  
cut -d, -f6 | sort | uniq -c | sort -nr
```

## Dependencies

this code is for python3 and depends on the py-radix module

pip3 install py-radix

## Process

1. fetch the repository

```
rsync --delete -az rpki.cnnic.cn::rpki cnnic/
```

2. extract list of resources per certificate

by hand:

```
$ openssl x509 \           -inform DER \           -noout \           -text  
\  
    -in ./cnnic/A9162E3D0000/Y1vTOT_M9475iEK4qDNi1UnlneM.cer
```

scripted:

```
./readwhichopenssl.py ./cnnic/A9162E3D0000/Y1vTOT_M9475iEK4qDNi1UnlneM.cer  
\  
    > ./Y1vTOT_M9475iEK4qDNi1UnlneM.inr.txt This generates data
```

of the form:

```
./Y1vTOT_M9475iEK4qDNi1UnlneM.cer,635BD3393FCCF78EF98842B8A833489549E59DE3,IPv6,2407:d480:::  
./Y1vTOT_M9475iEK4qDNi1UnlneM.cer,635BD3393FCCF78EF98842B8A833489549E59DE3,IPv6,2407:d580:::  
./Y1vTOT_M9475iEK4qDNi1UnlneM.cer,635BD3393FCCF78EF98842B8A833489549E59DE3,IPv6,2407:d680:::  
./Y1vTOT_M9475iEK4qDNi1UnlneM.cer,635BD3393FCCF78EF98842B8A833489549E59DE3,IPv6,2407:d780:::  
./Y1vTOT_M9475iEK4qDNi1UnlneM.cer,635BD3393FCCF78EF98842B8A833489549E59DE3,IPv6,2407:d880:::  
./Y1vTOT_M9475iEK4qDNi1UnlneM.cer,635BD3393FCCF78EF98842B8A833489549E59DE3,IPv6,2407:d980:::  
./Y1vTOT_M9475iEK4qDNi1UnlneM.cer,635BD3393FCCF78EF98842B8A833489549E59DE3,IPv6,2407:da80:::  
./Y1vTOT_M9475iEK4qDNi1UnlneM.cer,635BD3393FCCF78EF98842B8A833489549E59DE3,IPv6,2407:db80:::  
./Y1vTOT_M9475iEK4qDNi1UnlneM.cer,635BD3393FCCF78EF98842B8A833489549E59DE3,IPv6,2407:dc80:::
```

3. filter the prefixes by RIR delegated file to tag by opaque-id field

the python program uses 0.. index fields so the field is 3, not 4.

```
./delegfilter.py -s, -t cc,orgid -n 3 \  
  < Y1vTOT_M9475iEK4qDNIlUnlneM.inr.txt \  
  > Y1vTOT_M9475iEK4qDNIlUnlneM.inr.orgid.txt
```

This generates data of the form:

```
./Y1vTOT_M9475iEK4qDNIlUnlneM.cer,635BD3393FCCF78EF98842B8A833489549E59DE3,IPv6,2407:f680:::  
./Y1vTOT_M9475iEK4qDNIlUnlneM.cer,635BD3393FCCF78EF98842B8A833489549E59DE3,IPv6,2407:f780:::  
./Y1vTOT_M9475iEK4qDNIlUnlneM.cer,635BD3393FCCF78EF98842B8A833489549E59DE3,IPv6,2407:f880:::  
./Y1vTOT_M9475iEK4qDNIlUnlneM.cer,635BD3393FCCF78EF98842B8A833489549E59DE3,IPv6,2407:f980:::  
./Y1vTOT_M9475iEK4qDNIlUnlneM.cer,635BD3393FCCF78EF98842B8A833489549E59DE3,IPv6,2407:fa80:::  
./Y1vTOT_M9475iEK4qDNIlUnlneM.cer,635BD3393FCCF78EF98842B8A833489549E59DE3,IPv6,2407:fb80:::  
./Y1vTOT_M9475iEK4qDNIlUnlneM.cer,635BD3393FCCF78EF98842B8A833489549E59DE3,IPv6,2407:fc80:::  
./Y1vTOT_M9475iEK4qDNIlUnlneM.cer,635BD3393FCCF78EF98842B8A833489549E59DE3,IPv6,2407:fd80:::
```

4. collate by opaque-id, count..

cut uses 1.. index fields so the field on output is 6 not 5

```
cut -d, -f6 < Y1vTOT_M9475iEK4qDNIlUnlneM.inr.orgid.txt | \  
  sort | \  
  uniq -c |\  
  sort -nr \  
  > Y1vTOT_M9475iEK4qDNIlUnlneM.orgid.counts.txt
```