APRICOT 2022 / APNIC Routing Security SIG (2-MAR-2022)

Status of RPKI in Australia and New Zealand

Government Services and Critical Infrastructure

YMMV AS WE'RE STILL WORKING ON THE REPORT!

Author:
Terry Sweetser
"Data Engineer"
terry@rpki.dev

Sponsor:
Aftab Siddiqui
Internet Society
Siddiqui@isoc.org

Abstract or WHY?

- Australia has made ICT infrastructure “Critical” and the government now has “intervention” powers.
- Routing Security is not a new issue, it’s as old as BGP.
- Route hijacks and “Fat Fingers” Route Leaks are continuing to happen.
- Bad Actors, including “Sovereign Governments” are using poor Routing Security for crime and oppression.

Data Summary What?

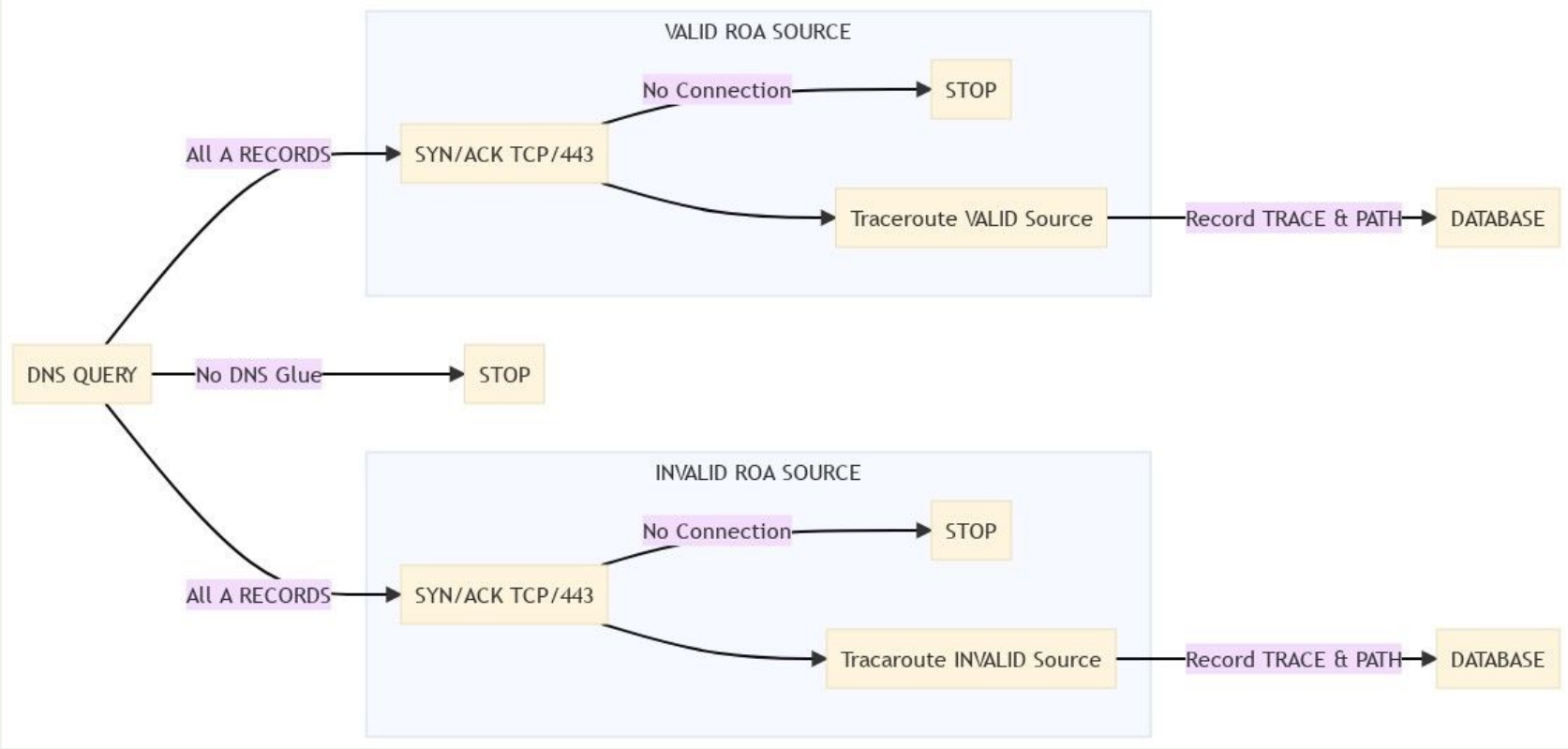
2,333,647 traceroutes
1,002,493 domains

AU NZ PK

school.nz govt.nz asn.au org.au net.pk edu.au com.au gos.pk org.pk net.nz co.nz org.nz id.au com.pk net.au gov.au edu.pk

Methodology: HOW?

Take all domains, get all A records, connect to port 443 on TCP, traceroute to all A records.



TRENDS:

- Some networks are very porous to invalid ROAs
- Some networks are 100% rejecting invalid ROAs traffic
- Some networks use bogons: returning ICMP traffic from bogons!

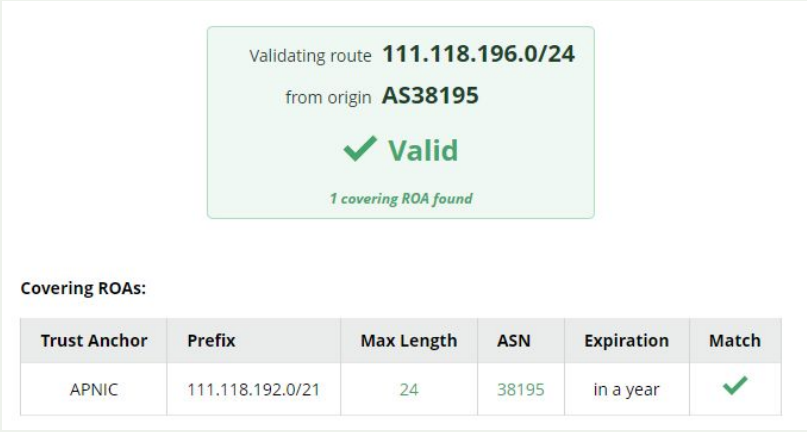
TESTS	VALID	INVALID	Domains	ASN	RATIO
1471	738	733	edu.au	55803	99.3%
1366	684	682	edu.au	45638	99.7%
1187	606	581	edu.au	15169	95.9%
1082	1082	0	edu.au	14618	0.0%
860	429	431	edu.au	45671	100.5%
833	435	398	gov.au	55532	91.5%
743	377	366	edu.au	4739	97.1%
553	553	0	edu.au	13335	0.0%
454	256	198	edu.au	38719	77.3%
384	384	0	gov.au	14618	0.0%
370	184	186	gov.au	20940	101.1%
312	164	148	edu.au	45768	90.2%
302	153	149	edu.au	9517	97.4%
295	142	153	edu.au	135543	107.7%
290	154	136	edu.au	9650	88.3%
285	136	149	gov.au	19551	109.6%
284	147	137	gov.au	56135	93.2%
247	111	136	edu.au	132680	122.5%
238	231	7	edu.au	16509	3.0%
236	236	0	gov.au	8075	0.0%
230	230	0	edu.au	8075	0.0%
221	221	0	gov.au	16509	0.0%
220	108	112	edu.au	27647	103.7%
214	111	103	edu.au	136557	92.8%
204	106	98	edu.au	26496	92.5%
192	92	100	edu.au	139344	108.7%
179	179	0	edu.au	20473	0.0%
171	171	0	gov.au	13335	0.0%
160	88	72	edu.au	7575	81.8%
160	95	65	edu.au	46606	68.4%

Figure 5 Test and Result counts for GOV.AU and EDU.AU per ASN (Source: Terry Sweetser)

Case Study: QLD.GOV.AU

```
project_pentest=# select * from invalid_rov_destinations where domain_id = 1839954;
 domain_id | traceroute_id | hop_id | route_id | cctld | second |    name    | source  | hop |     router      |      prefix      | asn |  as_name   | rir | reg_date | cc
-----------+---------------+--------+----------+-------+--------+------------+---------+-----+-----------------+------------------+-----+------------+-----+----------+----
   1839954 |           314 |   2780 |     1211 | au    | gov    | qld.gov.au | INVALID |   8 | 111.118.196.23  | 111.118.196.0/24 |   0 | Not Routed |     |          | XX
   1839954 |       1088665 |   2781 |     1211 | au    | gov    | qld.gov.au | VALID   |   9 | 111.118.196.29  | 111.118.196.0/24 |   0 | Not Routed |     |          | XX
   1839954 |           314 |   2781 |     1211 | au    | gov    | qld.gov.au | INVALID |   9 | 111.118.196.29  | 111.118.196.0/24 |   0 | Not Routed |     |          | XX
   1839954 |       1088665 |   2780 |     1211 | au    | gov    | qld.gov.au | VALID   |   8 | 111.118.196.23  | 111.118.196.0/24 |   0 | Not Routed |     |          | XX
(4 rows)
```

Is something rotten in the state of ~~Denmark~~ QLD?



Validating route **111.118.196.0/24**

from origin **AS38195**

✔ **Valid**

1 covering ROA found

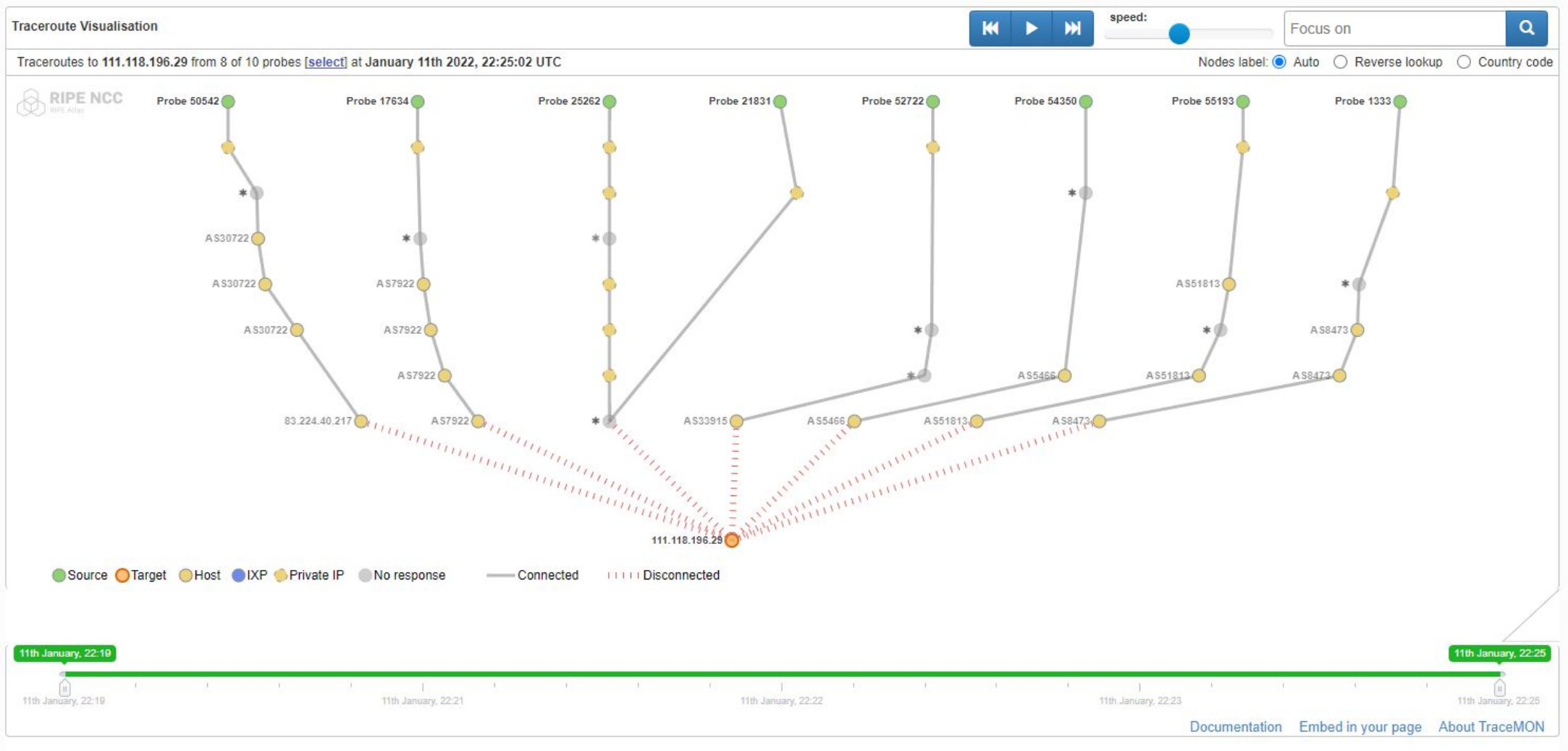
Covering ROAs:

Trust Anchor	Prefix	Max Length	ASN	Expiration	Match
APNIC	111.118.192.0/21	24	38195	in a year	✔

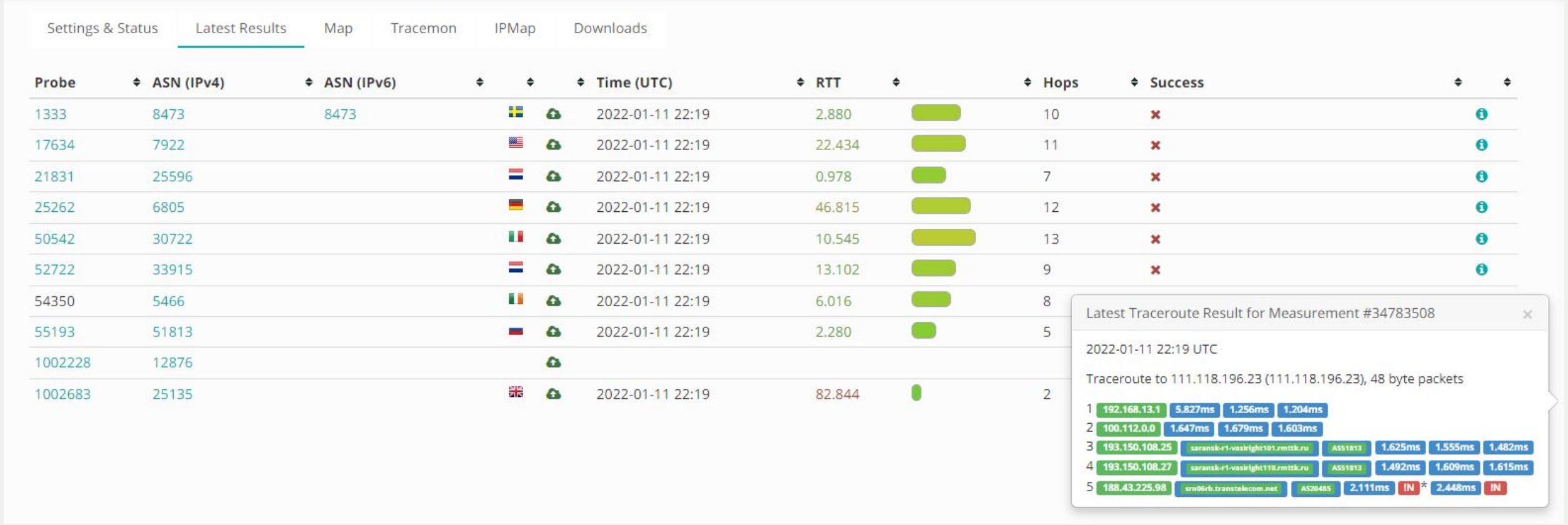
```
project_pentest=# \x
Expanded display is on.
project_pentest=# select * from ip_lookup_cache where id = 1211;
-[ RECORD 1 ]-------------------------
handle      | No AS
asn         | 0
as_name     | Not Routed
rir         |
reg_date    |
prefix      | 111.118.196.0/24
cc          | XX
domain      |
isp         |
data_source | ATLAS
created     | 2021-09-06 03:31:18.151426
updated     |
id          | 1211
rov         | INVALID
```

LOW PUBLIC DATA QUALITY?

Case Study: QLD.GOV.AU



Case Study: QLD.GOV.AU



https://atlas.ripe.net/measurements/34783508/#probes

Summary: So far so what?

- Transit ASs are still allowing traffic between invalids.
- BGP Filters are not enough: need to blackhole invalids.
- Public sources of data are not as good as they should be!

- Is Hot Potato routing fair and reasonable now?
- BCP38, as old as time, yet so rarely used?

Should multihomed clients accept 0/0 and ::/0 from you?

Questions?

Thank you.

Terry Sweetser
“Data Engineer”
terry@rpki.dev
about.me/terry.sweetser

Rue Vallin 2
CH-1201 Geneva
Switzerland

11710 Plaza America Drive
Suite 400
Reston, VA 20190, USA

Rambla Republica de Mexico 6125
11000 Montevideo,
Uruguay

66 Centrepoint Drive
Nepean, Ontario, K2G 6J5
Canada

Science Park 400
1098 XH Amsterdam
Netherlands

3 Temasek Avenue, Level 21
Centennial Tower
Singapore 039190

internetsociety.org
@internetsociety

PSA: SIGN YOUR ROUTES!

https://www.apnic.net/community/security/resource-certification/#routing