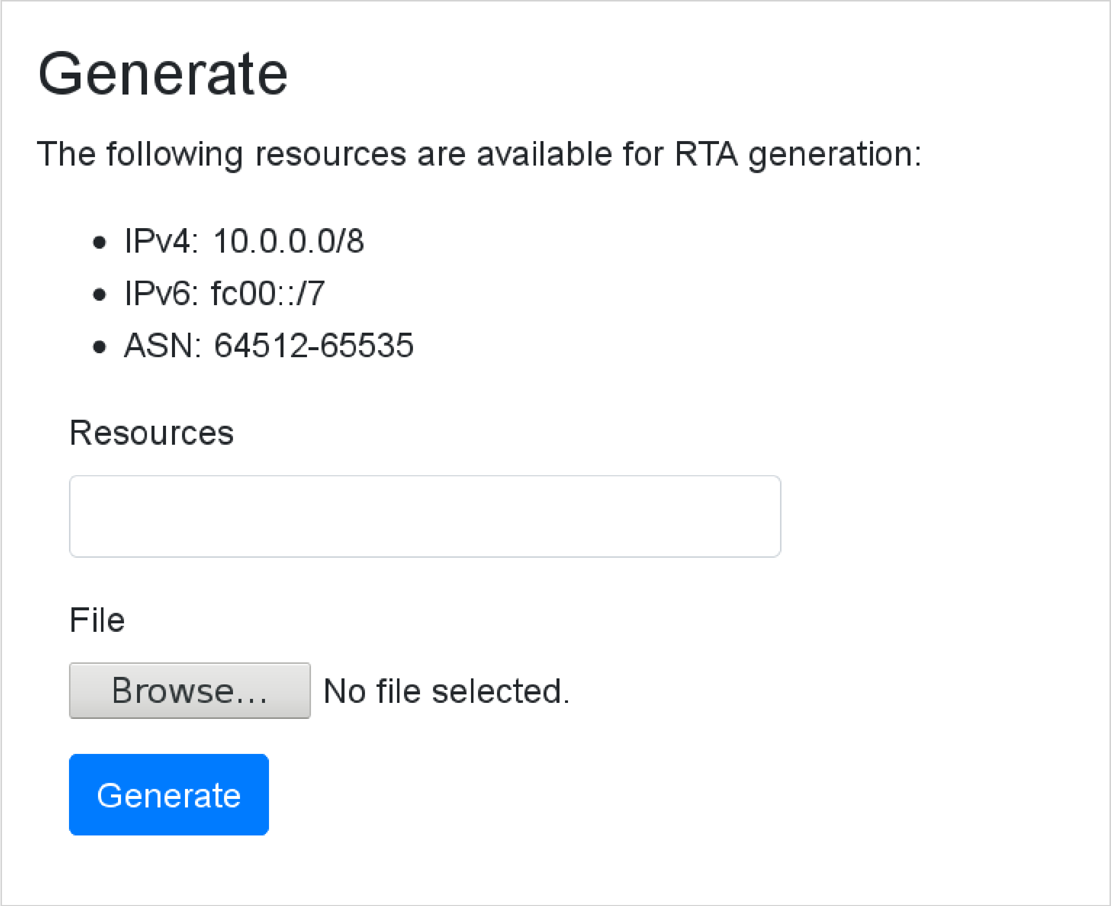
RPKI RTAs
RDAP Mirroring

APNIC Products and Services

What is an RPKI RTA? (1)

- **R**esource-**T**agged **A**ttestation
- The associated specification provides for:
  - signing an arbitrary file using an RPKI certificate;
  - packaging the signature and its certificate chain into an object (the **RTA** itself); and
  - verifying the signature (i.e. “this file was signed by the holder of address block 192.0.2.0/24”)



Generate

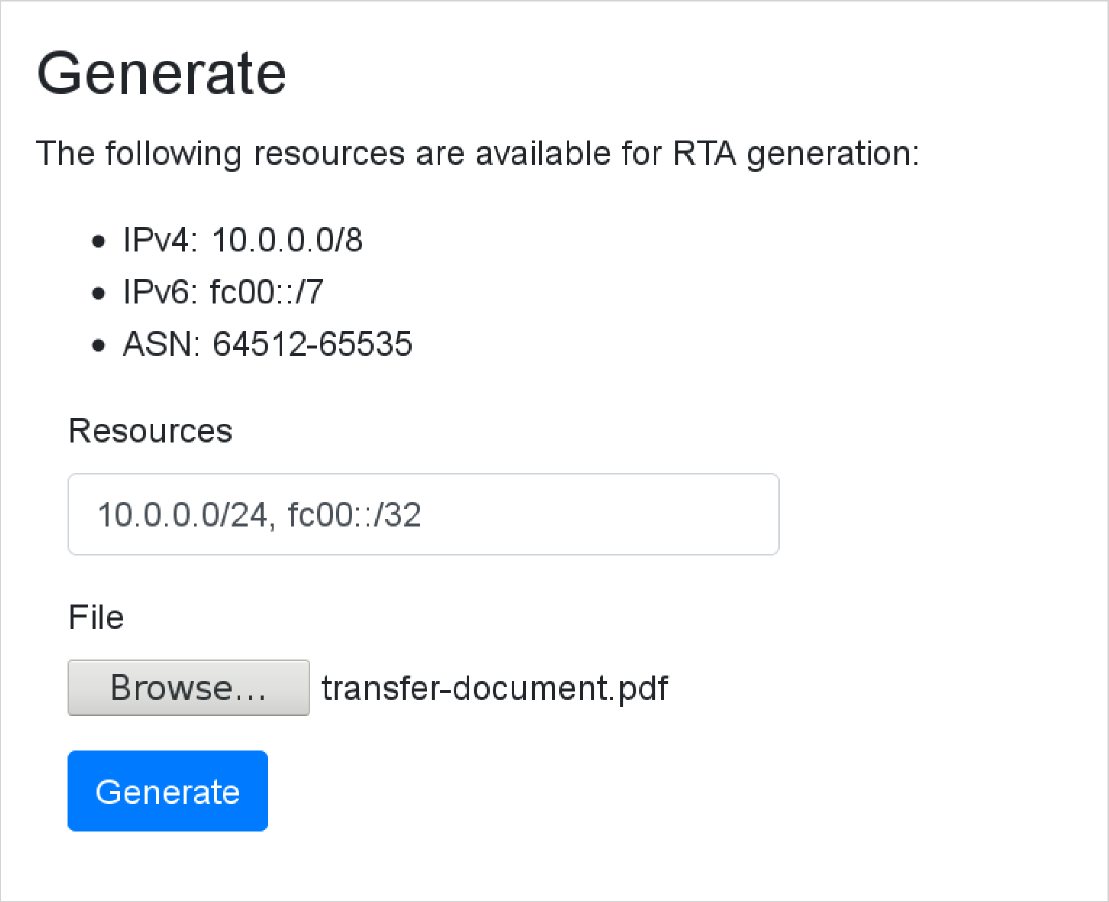
The following resources are available for RTA generation:

- IPv4: 10.0.0.0/8
- IPv6: fc00::/7
- ASN: 64512-65535

Resources

File

No file selected.



Generate

The following resources are available for RTA generation:

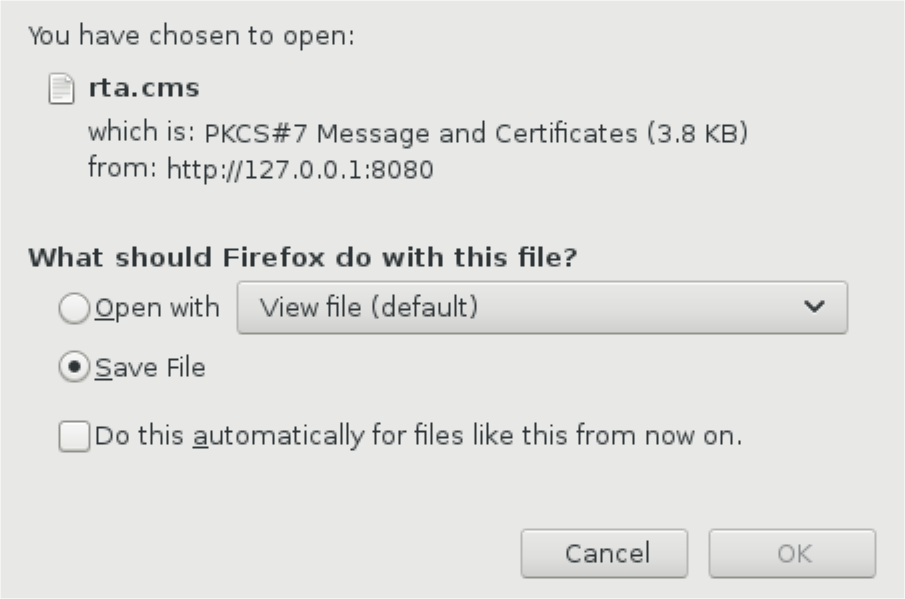
- IPv4: 10.0.0.0/8
- IPv6: fc00::/7
- ASN: 64512-65535

Resources

10.0.0.0/24, fc00::/32

File

transfer-document.pdf



You have chosen to open:

rta.cms

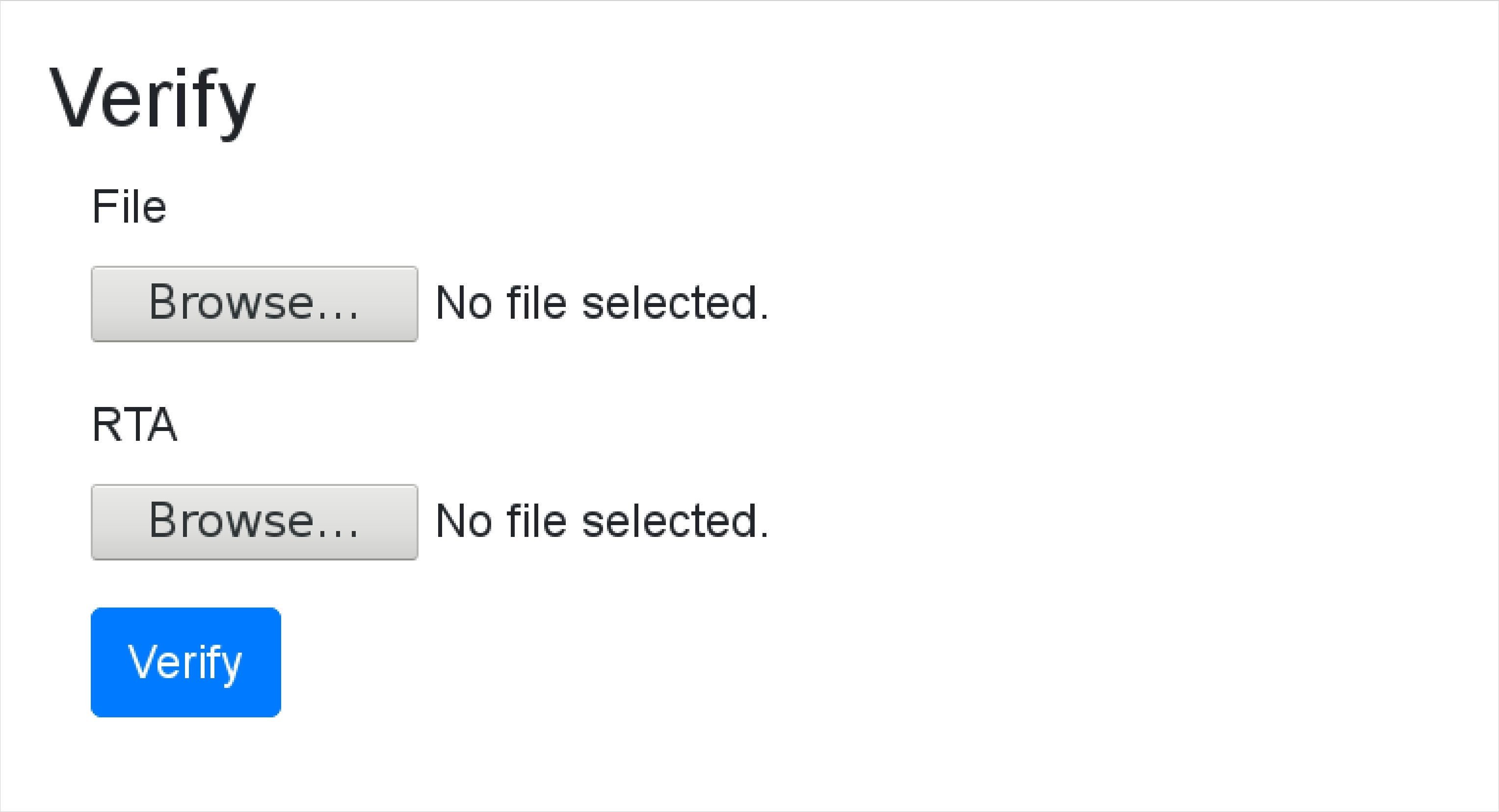
which is: PKCS#7 Message and Certificates (3.8 KB)
from: http://127.0.0.1:8080

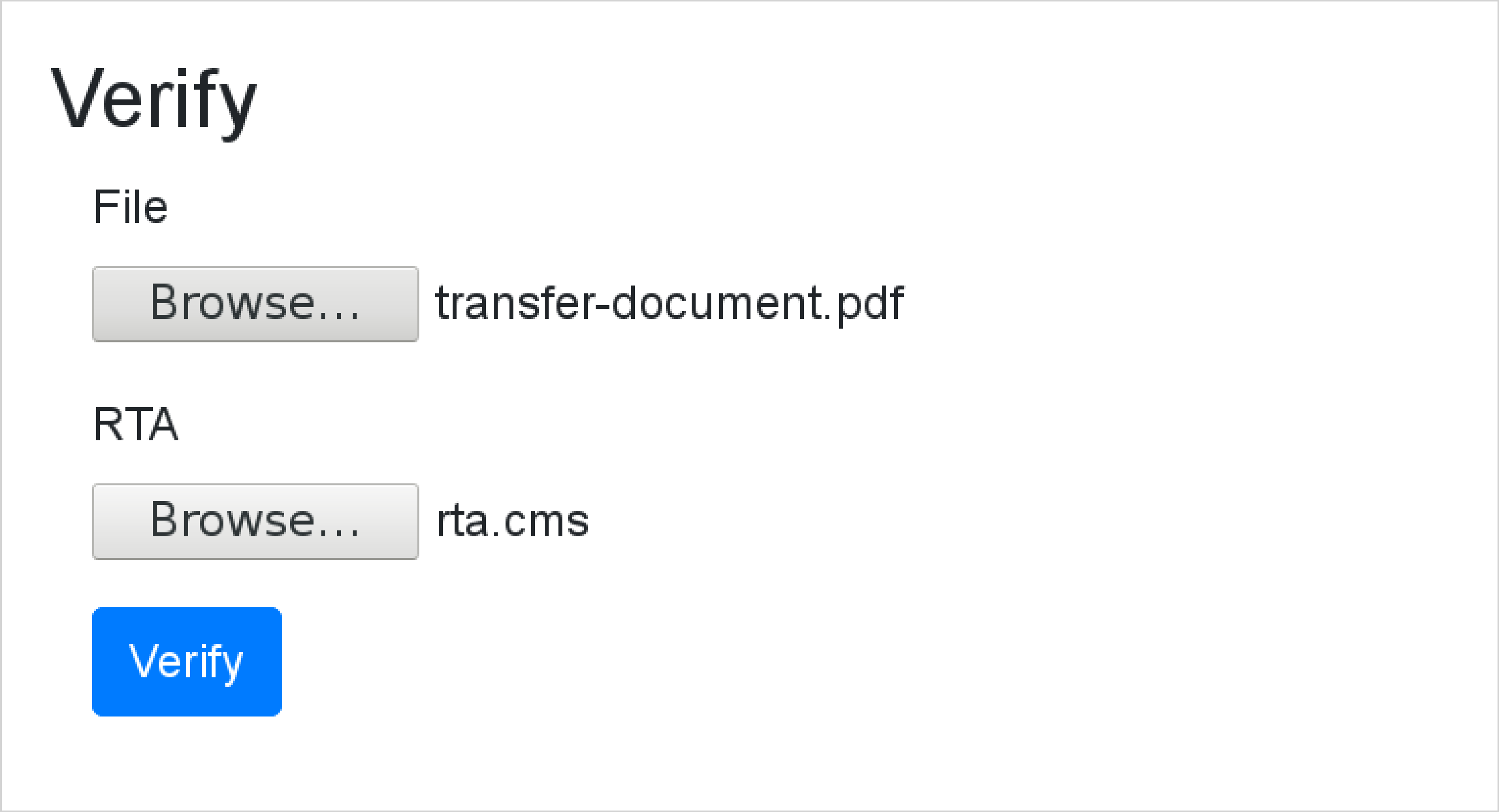
What should Firefox do with this file?

○ Open with

● Save File

□ Do this automatically for files like this from now on.


Verify
File
Browse...
No file selected.
RTA
Browse...
No file selected.
Verify



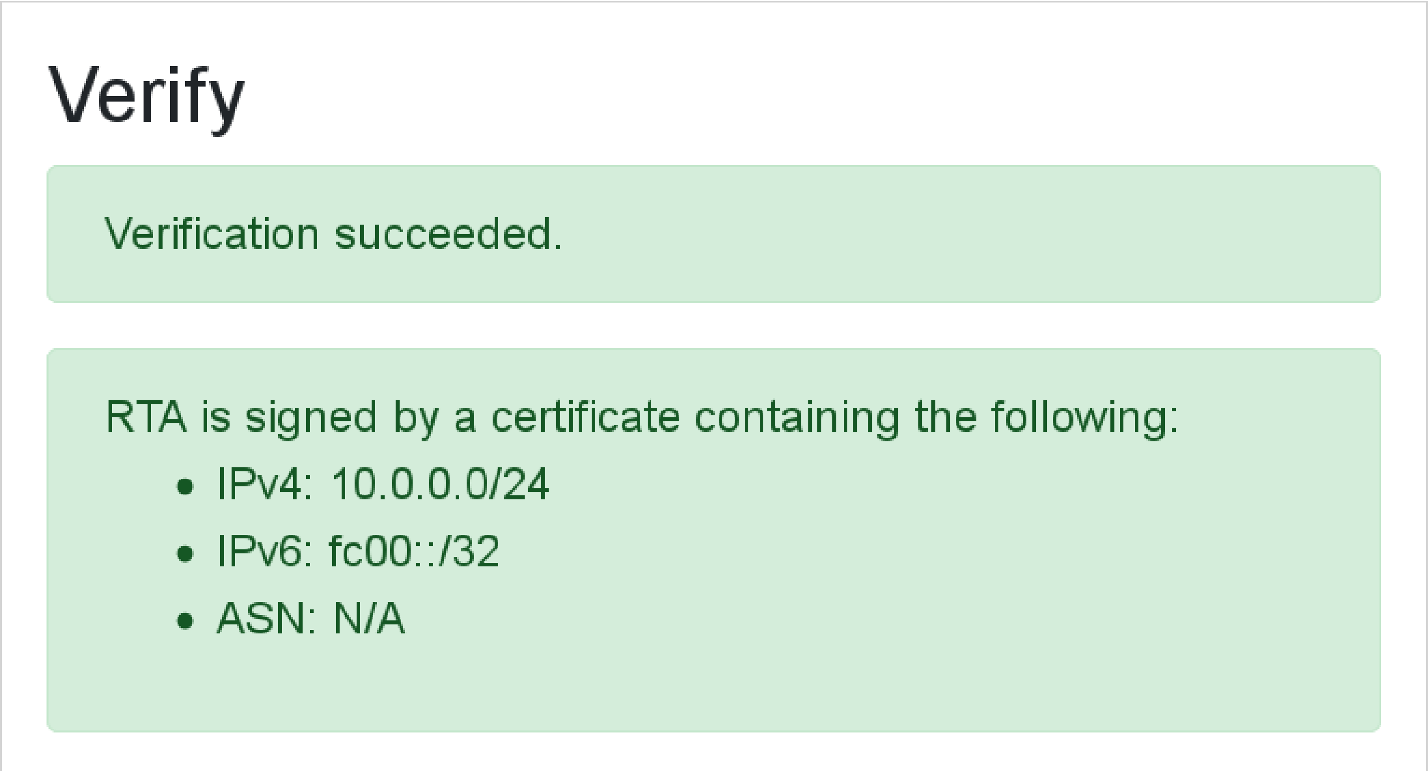
Verify

File

transfer-document.pdf

RTA

rta.cms



Verify

Verification succeeded.

RTA is signed by a certificate containing the following:

- IPv4: 10.0.0.0/24
- IPv6: fc00::/32
- ASN: N/A

Why is it useful?

- Arbitrary files can be signed
  - More flexible than existing RPKI functions
  - Supports ad hoc/people-driven processes
- RTAs do not have to be published
  - Associated business operations can remain private

Use cases for RTAs? (1)

- Letter of Authorization (LoA)
  - Some service providers require that resource holders give to them an LoA, signed by the registry that issued the resources, asserting that the holder is entitled to use those resources
- An RTA could be generated by the holder themselves to meet this requirement: no need for manual work by the registry

Use cases for RTAs? (2)

- Proof of control for the purposes of transfer
  - When transferring resources, work is required to establish that the source of the addresses actually controls the addresses that they are holding out for transfer
- Similarly to the previous use case, an RTA could be used by the holder to sign a statement indicating that they control the addresses and are willing to transfer them

Use cases for RTAs? (3)

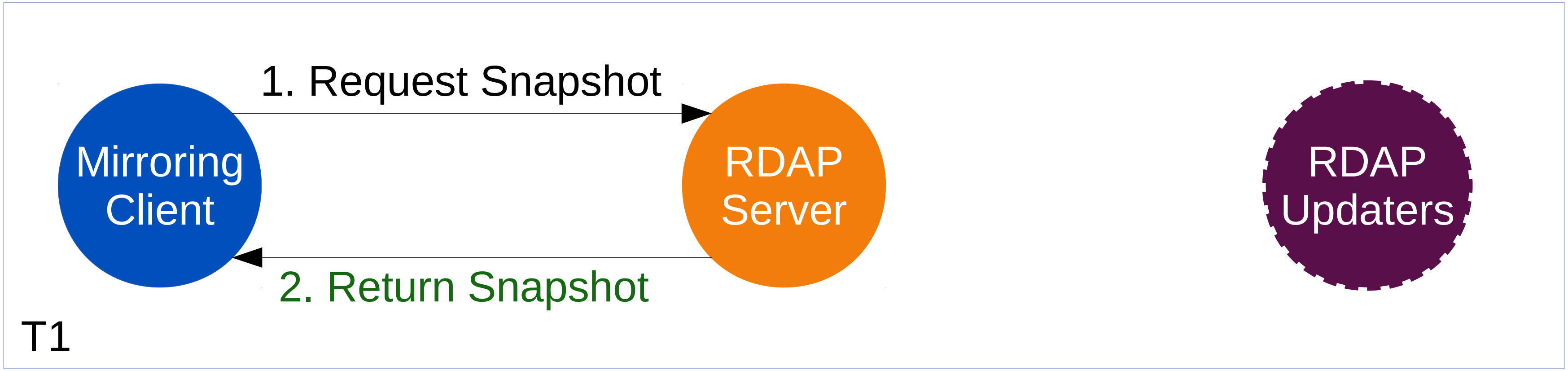
- By providing a more flexible and easy-to-deploy mechanism for making use of RPKI, RTAs will allow system developers to avoid less secure alternatives
- For example, there is an AWS feature called "Bring Your Own IP Addresses" (BYOIP), which relies on users making ad hoc updates to Whois records to demonstrate control
- RTAs will allow developers to rely on RPKI instead, which will typically improve the security characteristics of their services

Current status?

- Draft specification
  - https://tools.ietf.org/html/draft-michaelson-rpki-rta-00
- Proof-of-concept code
  - https://github.com/apnic-net/rpki-rta-demo
- Test UI for creating and validating RTAs
  - http://rpki-testbed.apnic.net/rta
- Feedback appreciated

What is RDAP Mirroring?

- A protocol for transferring bulk RDAP response data, and for keeping a local copy of that data up to date
- Client receives a ‘snapshot’ file from an RDAP service, containing all of that service’s current RDAP data
- Client then periodically retrieves ‘delta’ files from service, containing the changes that have happened since the snapshot was generated



1. Request Snapshot

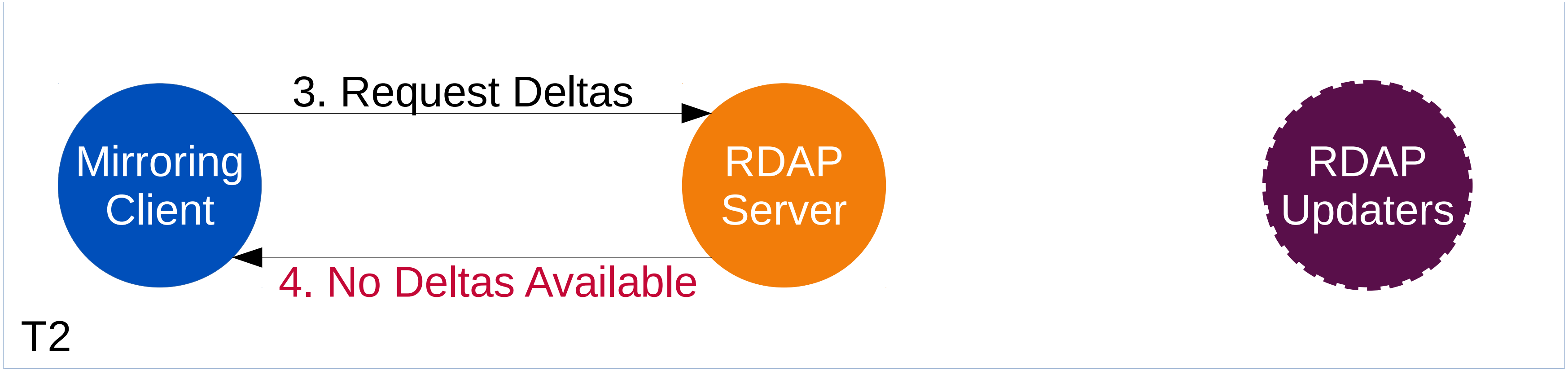
Mirroring Client

RDAP Server

RDAP Updaters

2. Return Snapshot

T1



3. Request Deltas

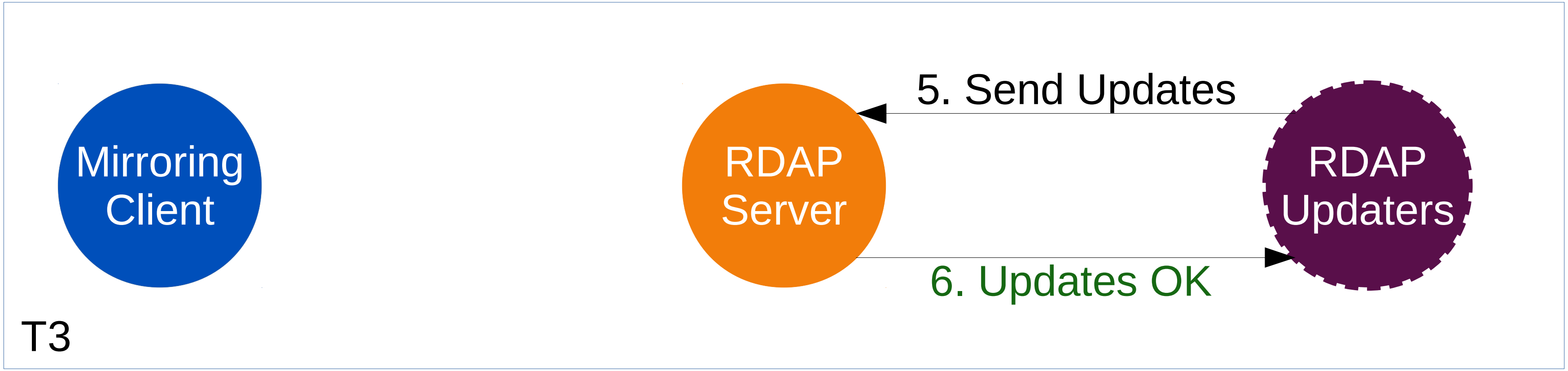
Mirroring Client

RDAP Server

RDAP Updaters

4. No Deltas Available

T2



Mirroring Client

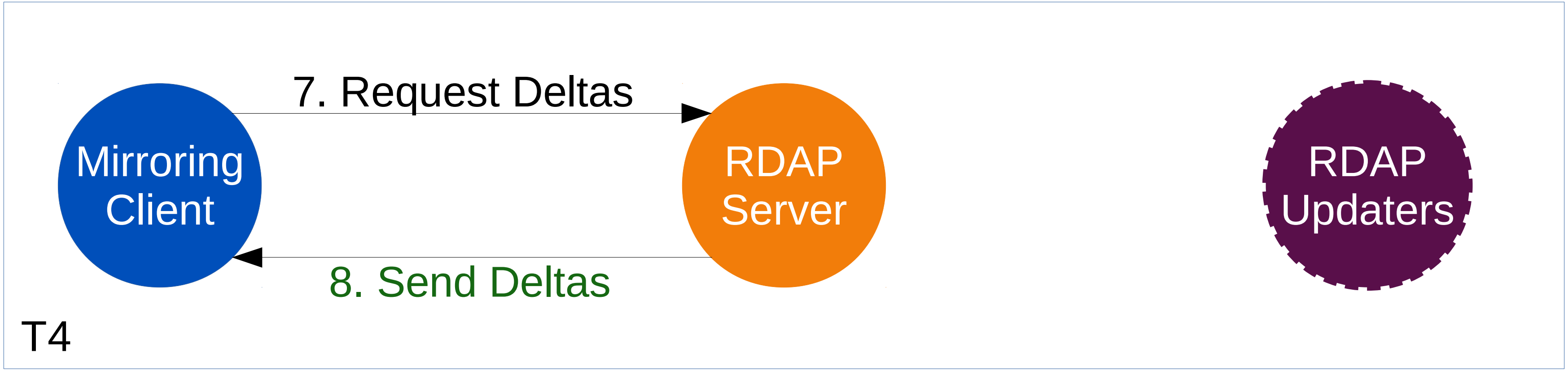
RDAP Server

RDAP Updaters

5. Send Updates

6. Updates OK

T3



Mirroring Client

RDAP Server

RDAP Updaters

7. Request Deltas

8. Send Deltas

T4

Why is it useful? (1)

- When the overhead of querying a remote RDAP server is too high: having a local copy of the data avoids this problem
- When there’s a need to analyse the RDAP data set as a whole, especially on an ongoing basis
- When a client wants to provide access in their own right to the remote RDAP server’s data

Why is it useful? (2)

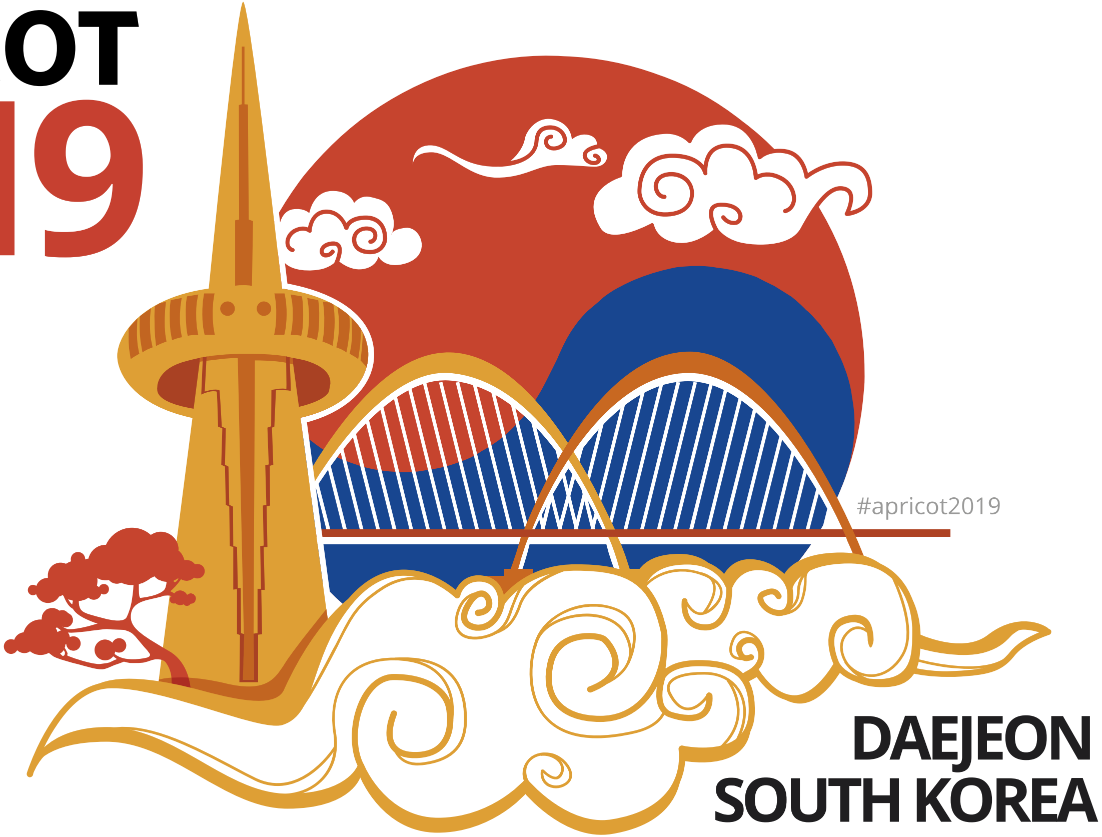
- The main motivation for APNIC is the third use case
- APNIC currently serves NIR Whois data from whois.apnic.net, but this data is English-language only
- With RDAP mirroring, NIRs can provide both English- and local-language data to us, which will help to make APNIC's RDAP service more accessible/usable for a wider audience

Current status?

- Draft specification:
  - https://tools.ietf.org/html/draft-harrison-regext-rdap-mirroring-00
- No proof-of-concept code available as yet
- Feedback appreciated

APRICOT 2019

APNIC 47



#apricot2019

DAEJEON
SOUTH KOREA
18 – 28 February 2019