ARIN + NANOG

ON THE ROAD

Waterloo, ON

Sept 2016

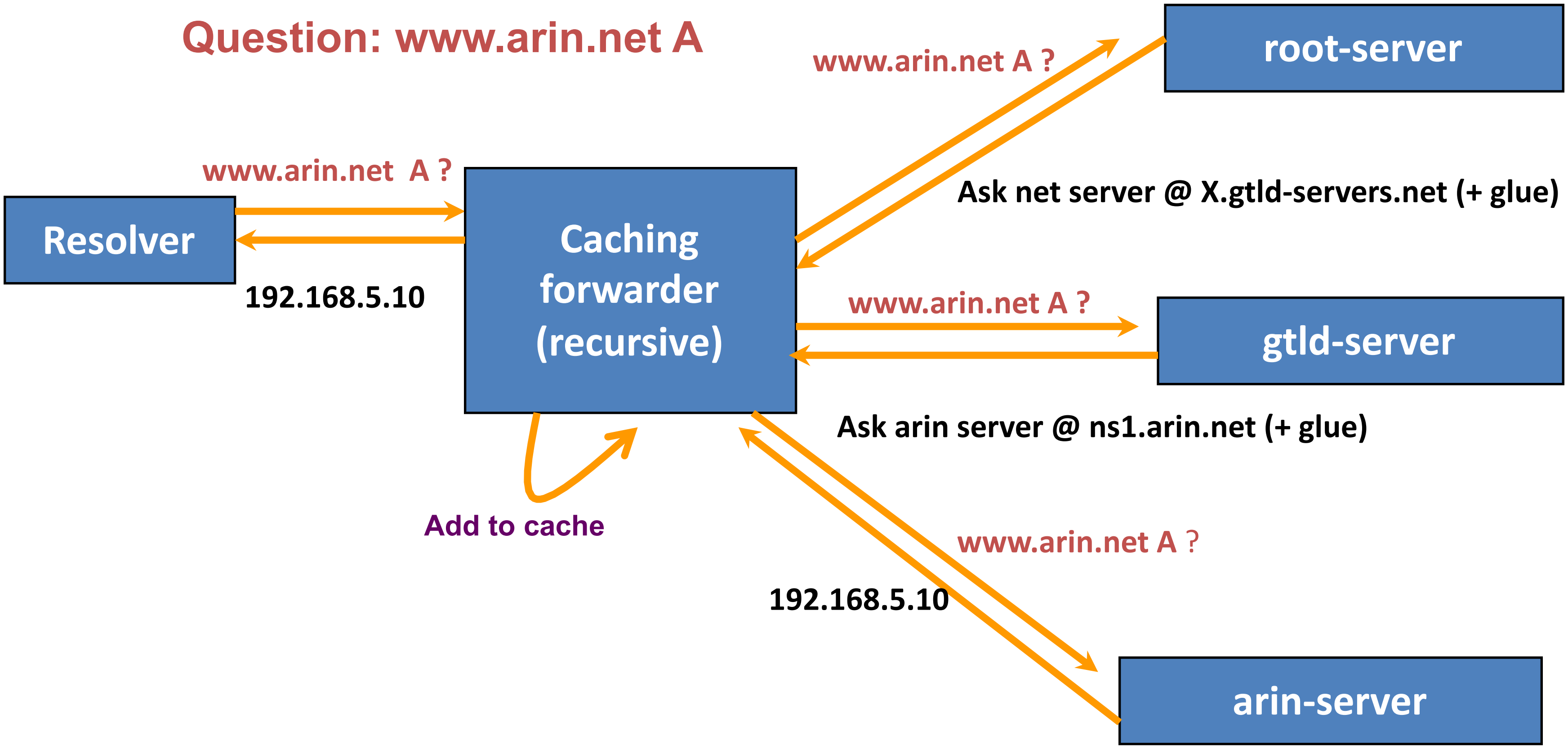
Core Internet Protocols

- **Two critical resources that are unsecured**
  - Domain Name Servers
  - Routing
- **Hard to tell if compromised**
  - From the user point of view
  - From the ISP/Enterprise

DNS

How DNS Works

Question: www.arin.net A



Resolver

www.arin.net A ?

192.168.5.10

Caching forwarder (recursive)

Add to cache

root-server

www.arin.net A ?

Ask net server @ X.gtld-servers.net (+ glue)

gtld-server

www.arin.net A ?

Ask arin server @ ns1.arin.net (+ glue)

arin-server

www.arin.net A ?

192.168.5.10

Why DNSSEC? What is it?

- Standard DNS (forward or reverse) responses are not secure
  - Easy to spoof
  - Notable malicious attacks
- DNSSEC attaches signatures
  - Validates responses
  - Can not spoof

Reverse DNS at ARIN

- ARIN issues blocks without any working DNS
  - Registrant must establish delegations after registration
  - Then employ DNSSEC if desired
- Just as susceptible as forward DNS if you do not use DNSSEC

Reverse DNS at ARIN

- Authority to manage reverse zones follows allocations
  - “Shared Authority” model
  - Multiple sub-allocation recipient entities may have authority over a particular zone

Changes completed to make DNSSEC work at ARIN

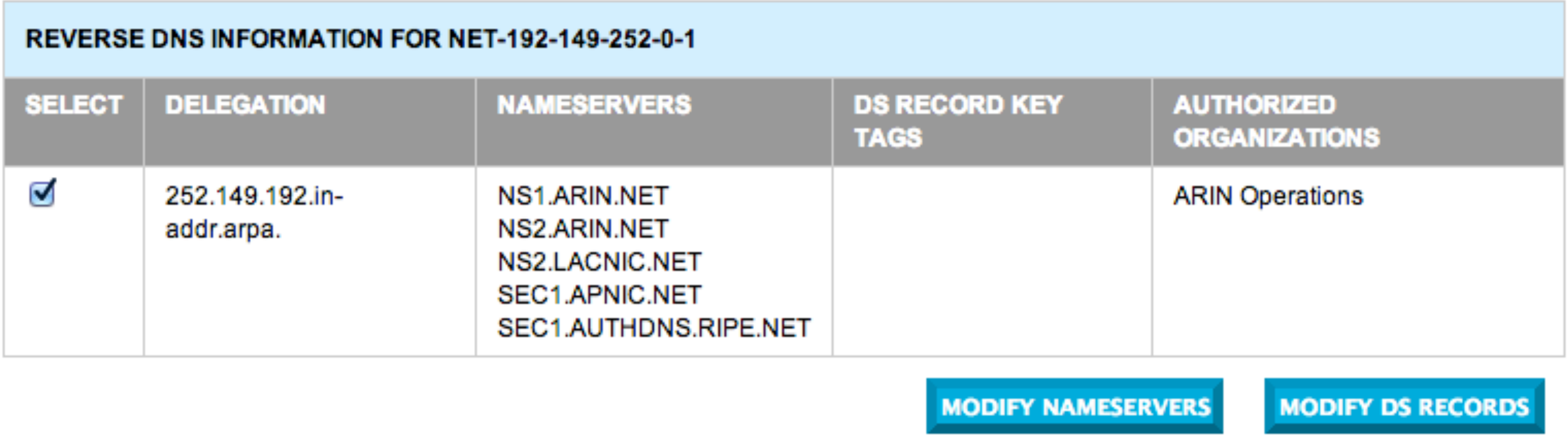
- Permit by-delegation management
- Sign in-addr.arpa. and ip6.arpa. delegations that ARIN manages
- Create entry method for DS Records
  - ARIN Online
  - RESTful interface
  - Not available via templates

Changes completed to make DNSSEC work at ARIN

- Key holders create and submit Delegation Signer (DS) records after securing their zones locally
- DNSSEC users ***should*** have signed a registration services agreement with ARIN to use these services

Reverse DNS in ARIN Online

First identify the network that you want to put Reverse DNS nameservers on…

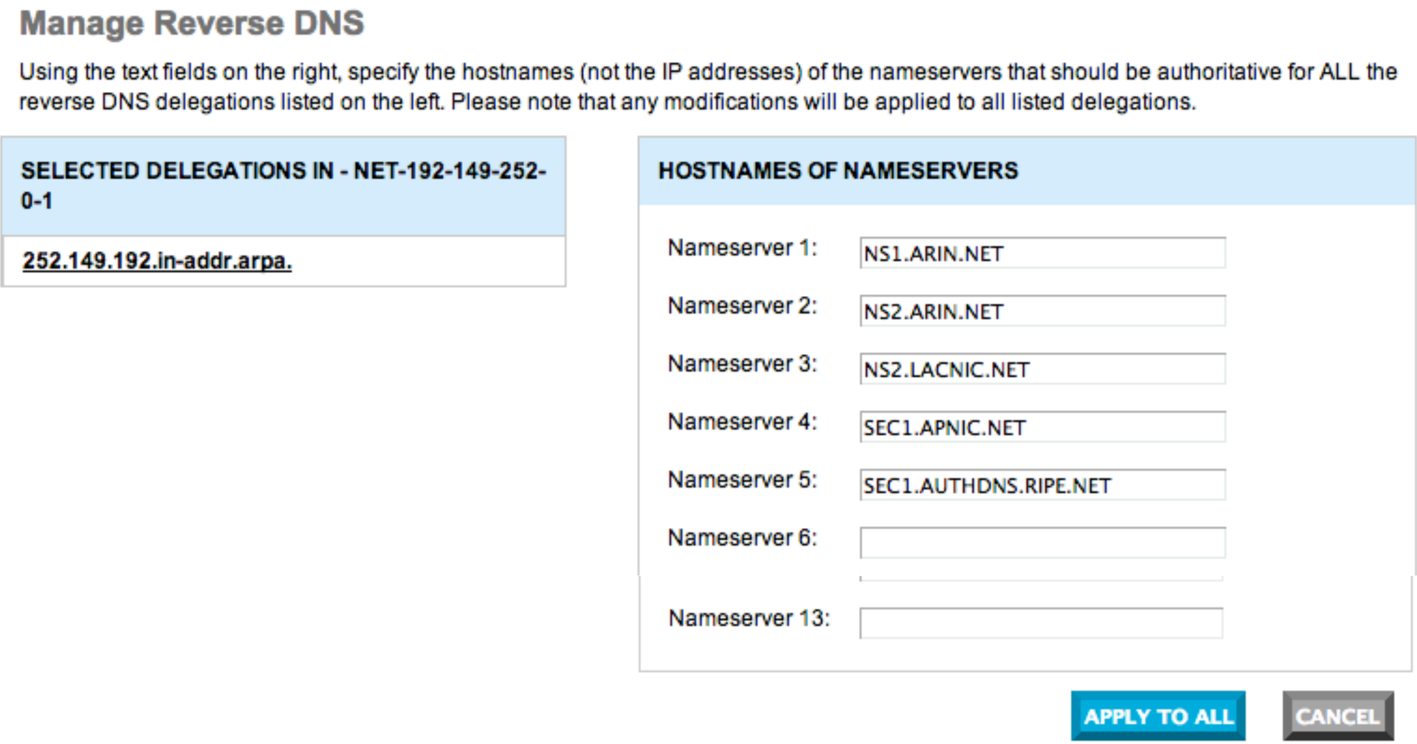


REVERSE DNS INFORMATION FOR NET-192-149-252-0-1

SELECT	DELEGATION	NAMESERVERS	DS RECORD KEY TAGS	AUTHORIZED ORGANIZATIONS
☑	252.149.192.in-addr.arpa.	NS1.ARIN.NET NS2.ARIN.NET NS2.LACNIC.NET SEC1.APNIC.NET SEC1.AUTHDNS.RIPE.NET		ARIN Operations

Reverse DNS in ARIN Online

…then enter the Reverse DNS nameservers…



Manage Reverse DNS

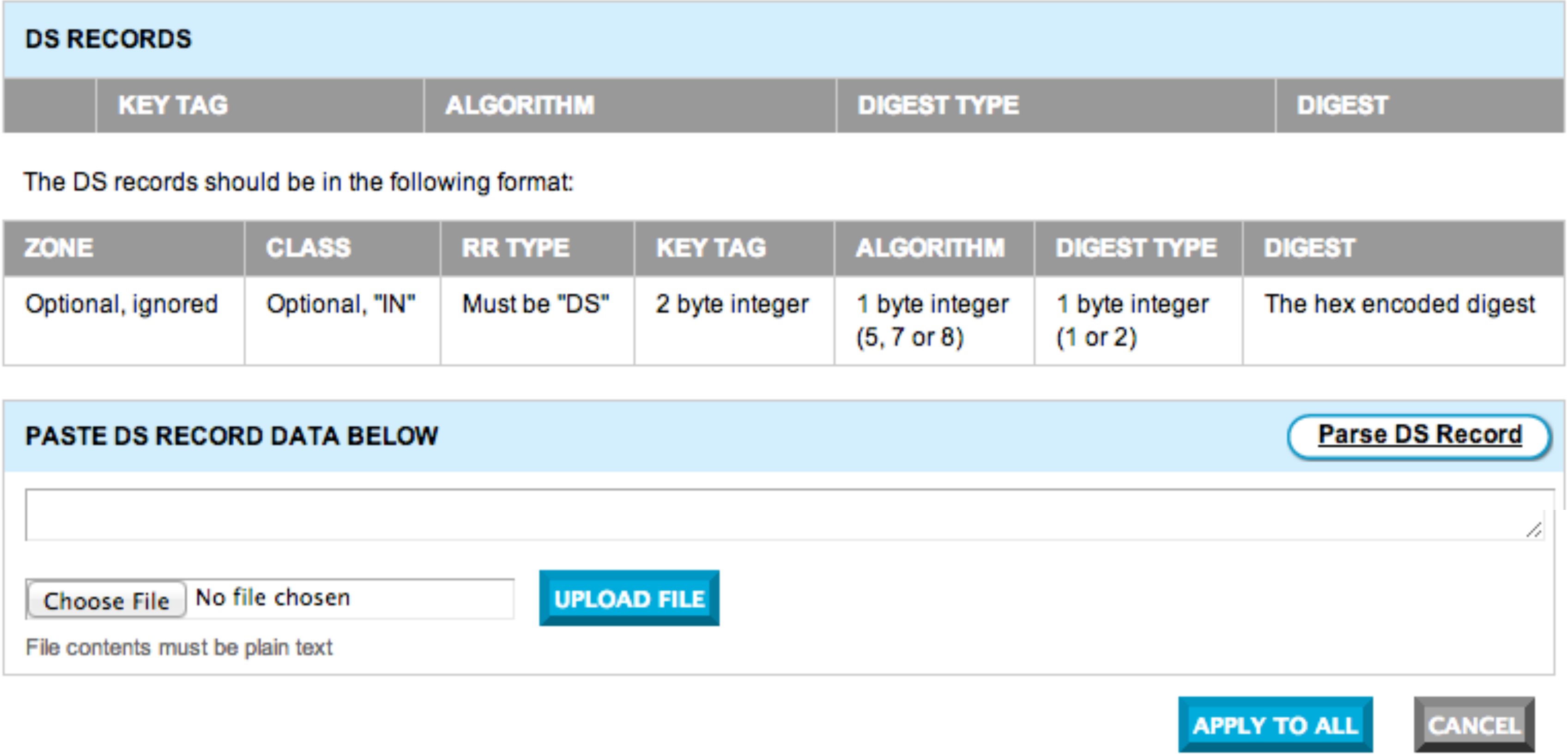
Using the text fields on the right, specify the hostnames (not the IP addresses) of the nameservers that should be authoritative for ALL the reverse DNS delegations listed on the left. Please note that any modifications will be applied to all listed delegations.

SELECTED DELEGATIONS IN - NET-192-149-252-0-1
252.149.192.in-addr.arpa.

HOSTNAMES OF NAMESERVERS	
Nameserver 1:	NS1.ARIN.NET
Nameserver 2:	NS2.ARIN.NET
Nameserver 3:	NS2.LACNIC.NET
Nameserver 4:	SEC1.APNIC.NET
Nameserver 5:	SEC1.AUTHDNS.RIPE.NET
Nameserver 6:	
Nameserver 13:	

DNSSEC in ARIN Online

…then apply DS record to apply to the delegation



DS RECORDS

	KEY TAG	ALGORITHM	DIGEST TYPE	DIGEST

The DS records should be in the following format:

ZONE	CLASS	RR TYPE	KEY TAG	ALGORITHM	DIGEST TYPE	DIGEST
Optional, ignored	Optional, "IN"	Must be "DS"	2 byte integer	1 byte integer (5, 7 or 8)	1 byte integer (1 or 2)	The hex encoded digest

PASTE DS RECORD DATA BELOW

No file chosen

File contents must be plain text

Reverse DNS: Querying ARIN’s Whois

Query for the zone directly:

```
Whois> whois -h whois.arin.net 136.136.192.in-addr.arpa

Name:           252.149.192.in-addr.arpa.
Updated:        2014-08-20
NameServer:     SEC1.APNIC.NET
NameServer:     NS1.ARIN.NET
NameServer:     NS2.LACNIC.NET
NameServer:     SEC1.AUTHDNS.RIPE.NET
NameServer:     NS2.ARIN.NET
KeyTag:         18508
Algorithm:      5
DigestType:     1
Digest:         84A741F15E878A088F3884EBE1F0E56EA8599295
KeyTag:         18508
Algorithm:      5
DigestType:     2
Digest:
A9B8659C7795166863DE6FEC47808B58ED0CC6ADB0AA5E25B8F46FE87D3D7CBA
Ref:            https://whois.arin.net/rest/rdns/252.149.192.in-addr.arpa.
```

DNSSEC in Zone Files

```
; File written on Mon Feb 24 17:00:53 2014
; dnssec_signzone version 9.3.6-P1-RedHat-9.3.6-20.P1.el5_8.6
0.74.in-addr.arpa.      86400   IN NS   NS3.COVAD.COM.
                        86400   IN NS   NS4.COVAD.COM.
                        10800   NSEC    1.74.in-addr.arpa. NS RRSIG NSEC
                        10800   RRSIG   NSEC 5 4 10800 20140306210053 (
                                        20140224210053 57974 74.in-addr.arpa.
                                        oNk3GVaCWj2j8+EAr0PncqnZeQjm8h4w51nS
                                        D2VUi7YtR9FvYLF/j4KO+8qYZ3TAixb9c05c
                                        8EVIhtY1grXEdOm30zJpZyaoaODpbHt8FdWY
                                        vwup9Tq4oVbxVyuSNXriZ2Mq55IIMgDR3nAT
                                        BLP5UClxUWkgvS/6poF+W/1H4QY= )
1.74.in-addr.arpa.      86400   IN NS   NS3.COVAD.COM.
                        86400   IN NS   NS4.COVAD.COM.
                        10800   NSEC    10.74.in-addr.arpa. NS RRSIG NSEC
                        10800   RRSIG   NSEC 5 4 10800 20140306210053 (
                                        20140224210053 57974 74.in-addr.arpa.
                                        DKYGzSDtIypDVcer5e+XuwoDW4auKy6G/OCV
                                        VTcfQGk+3iyy2CEKOZuMZXFaaDvXnaxey9R1
                                        mjams519Ghxp2qOnnkOw6iB6mR5cNkYlkL0h
                                        lu+IC4Buh6DqM4HbJCZcMXKEtWE0a6dMf+tH
                                        sa+5OV7ezX5LCuDvQVp6p0LftAE= )
```

DNSSEC in Zone Files

```
0.121.74.in-addr.arpa.  86400   IN NS   DNS1.ACTUSA.NET.
                        86400   IN NS   DNS2.ACTUSA.NET.
                        86400   IN NS   DNS3.ACTUSA.NET.
                        86400   DS      46693 5 1 (
                                        AEEDA98EE493DFF5F3F33208ECB0FA4186BD
                                        8056 )
                        86400   DS      46693 5 2 (
                                        66E6D421894AFE2AF0B350BD8F4C54D2EBA5
                                        DA72A615FE64BE8EF600C6534CEF )
                        86400   RRSIG   DS 5 5 86400 20140306210053 (
                                        20140224210053 57974 74.in-addr.arpa.
                                        n+aPxBHuf+sbzQN4LmHzlOi0C/hkaSVO3q1y
                                        6J0KjqNPzYqtxLgZjU+IL9qhtIOocgNQib9l
                                        gFRmZ9inf2bER435GMsa/nnjpVVWW/MBRKxf
                                        Pcc72w2iOAMu2G0prtVT08ENxtu/pBfnsOZK
                                        nhCY8UOBOYLOLE5Whtk3XOuX9+U= )
                        10800   NSEC    1.121.74.in-addr.arpa. NS DS RRSIG
NSEC
                        10800   RRSIG   NSEC 5 5 10800 20140306210053 (
                                        20140224210053 57974 74.in-addr.arpa.
                                        YvRowkdVDfv+PW42ySNUwW8S8jRyV6EKKRxe
…
```

DNSSEC Validating Resolvers

- www.internetsociety.org/deploy360/dnssec/
- www.isc.org/downloads/bind/dnssec/

DNSSEC Statistics

	Sept 7, 2016
Number of Orgs with DNSSEC	137
Total Number of Delegations	602,230
DNSSEC Secured Zones	628
Percentage Secured	0.1 %

Reverse DNS Management and DNSSEC in ARIN Online

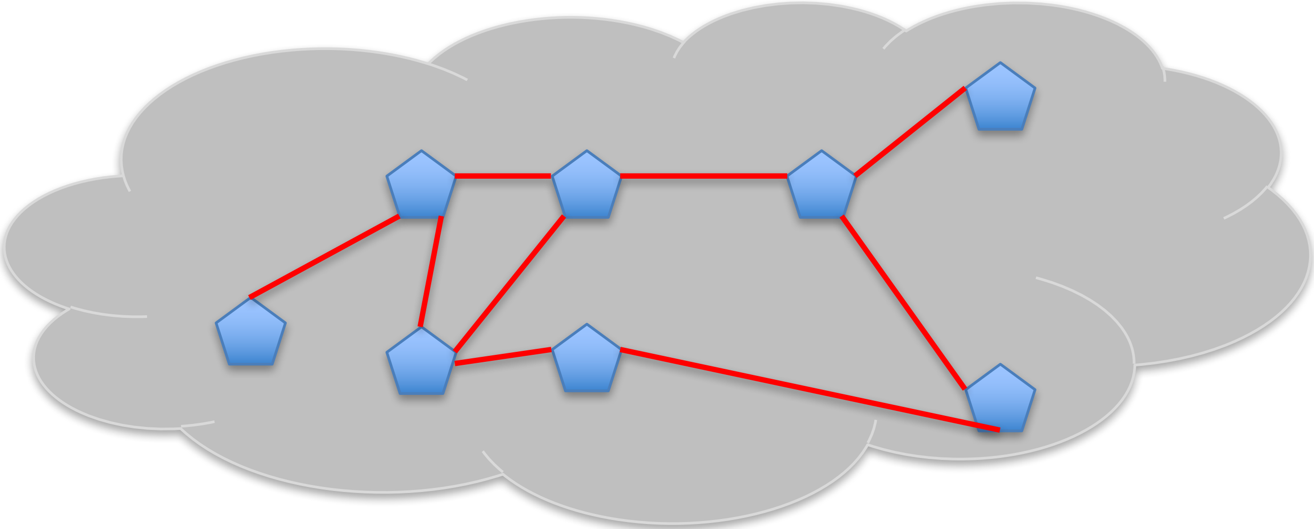
- Available on ARIN's website

http://www.arin.net/knowledge/dnssec/

Routing

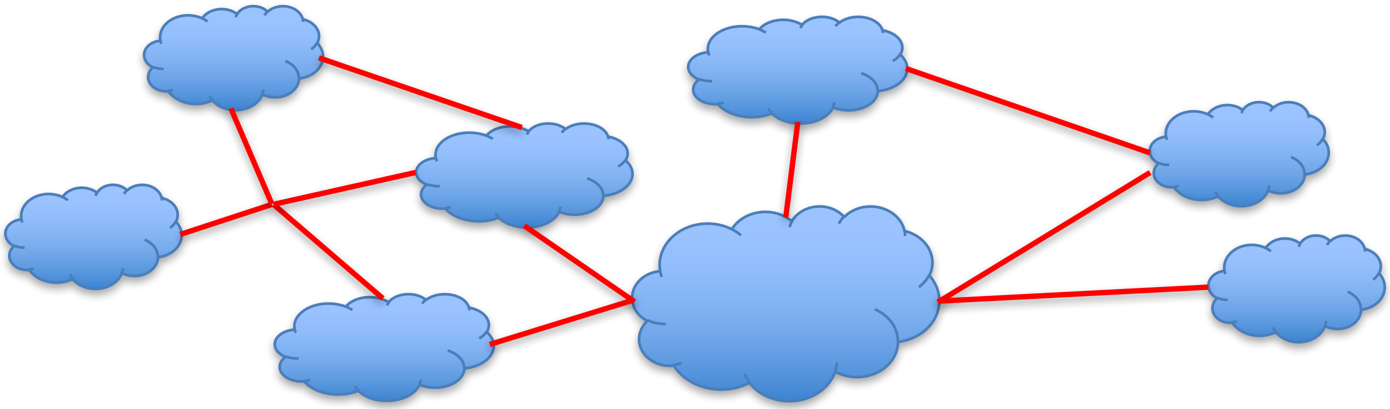
Routing Architecture

- The Internet uses a *two level* routing hierarchy:
  - **Interior** Routing Protocols, used by each network to determine how to reach all destinations that line within the network
  - **Interior** Routing protocols maintain the current topology of the network



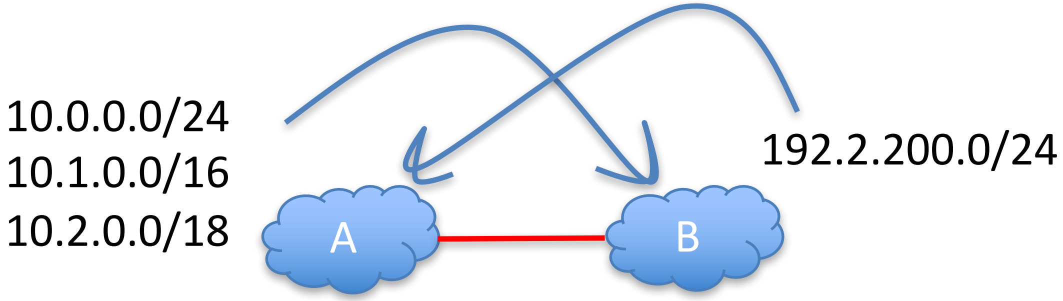
Routing Architecture

- The Internet uses a *two level* routing hierarchy:
  - **Exterior** Routing Protocol, used to link each component network together into a single whole
  - **Exterior** protocols assume that each network is fully interconnected internally



Exterior Routing: BGP

- BGP is a large set of bilateral (1:1) routing sessions
  - A tells B all the destinations (prefixes) that A is capable of reaching
  - B tells A all the destinations that B is capable of reaching



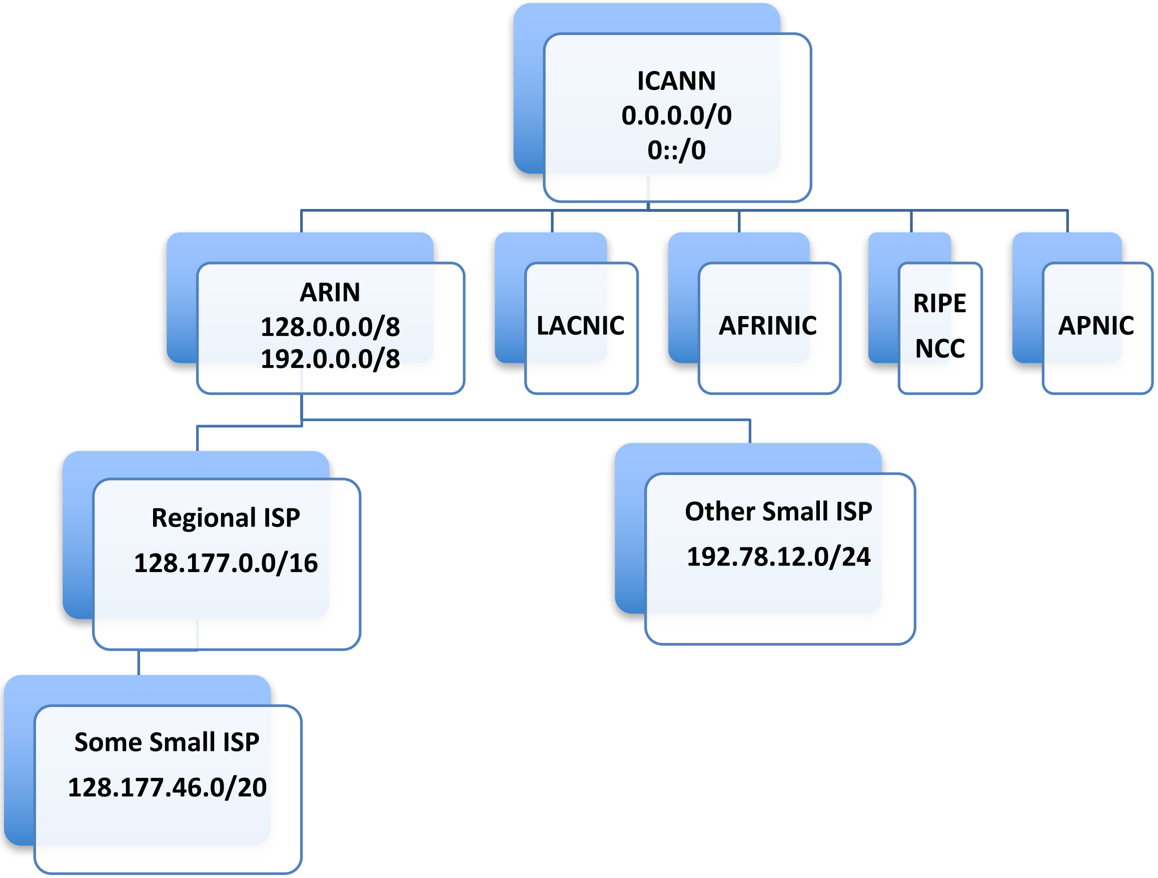
What is RPKI?

- **R**esource **P**ublic **K**ey **I**nfrastructure
- Attaches digital certificates to network resources
  - AS Numbers
  - IP Addresses
- Allows ISPs to associate the two
  - Route Origin Authorizations (ROAs)
  - Can follow the address allocation chain to the top

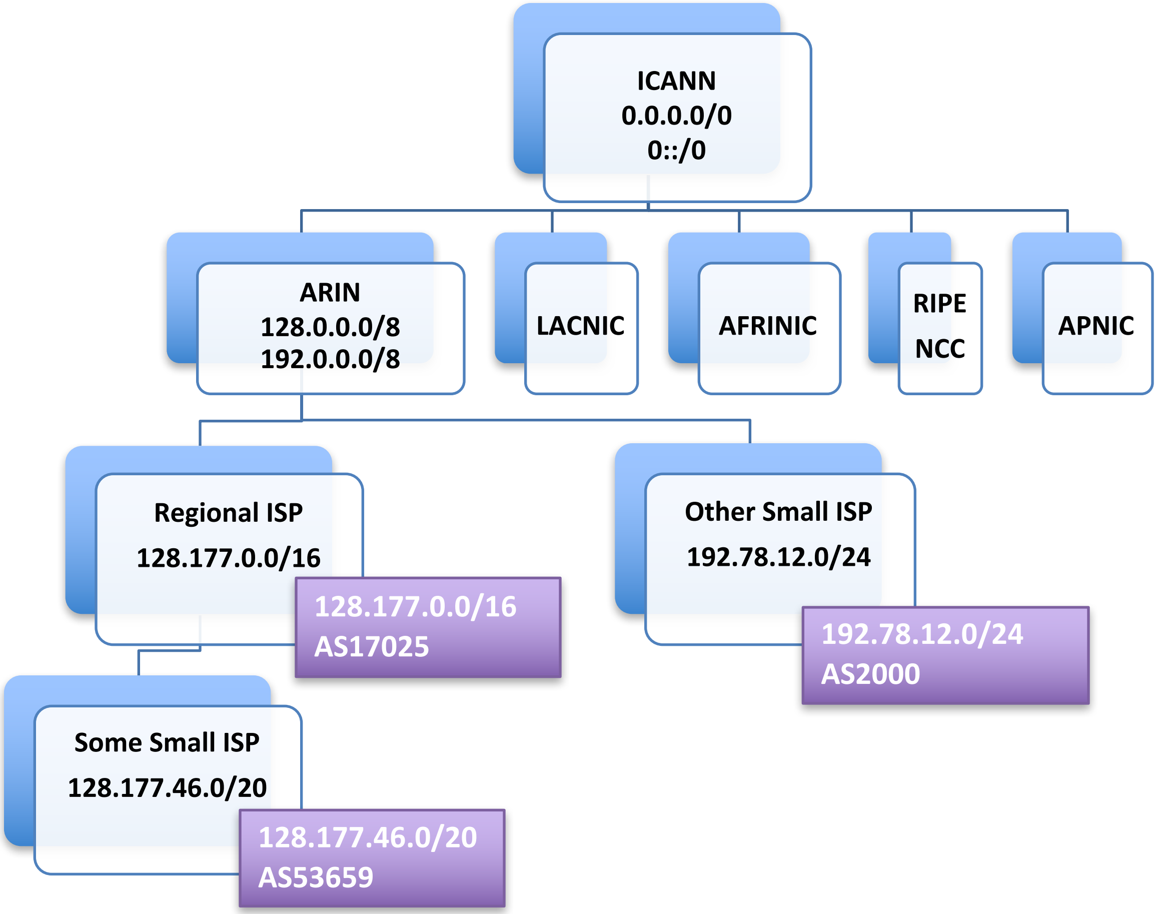
What does RPKI accomplish?

- Allows routers or other processes to validate route origins
- Simplifies validation authority information
  - Trust Anchor Locator
- Distributes trusted information
  - Through repositories

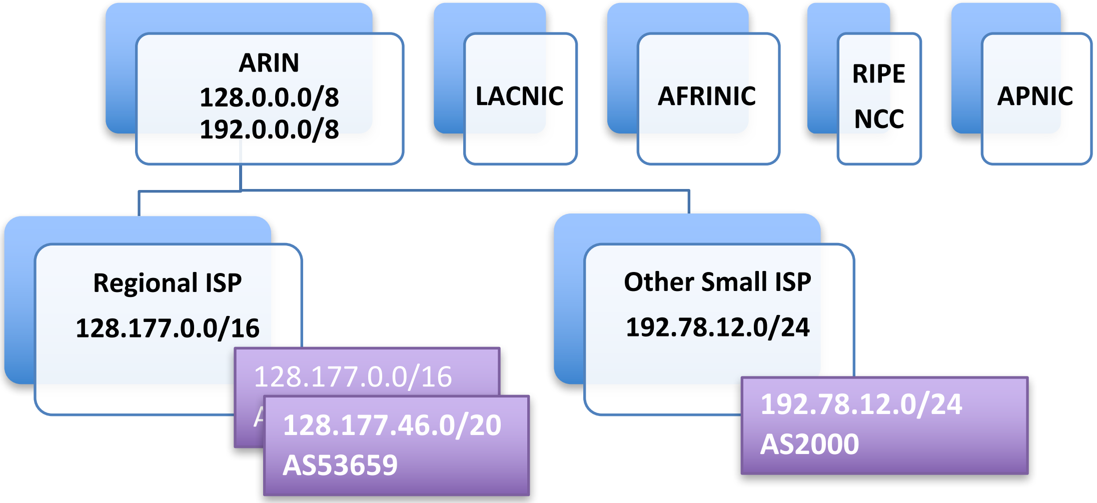
Hierarchy of Resource Certificates



Route Origin Attestations



Current Practices



ARIN
128.0.0.0/8
192.0.0.0/8

LACNIC

AFRINIC

RIPE
NCC

APNIC

Regional ISP
128.177.0.0/16

128.177.0.0/16
A

128.177.46.0/20
AS53659

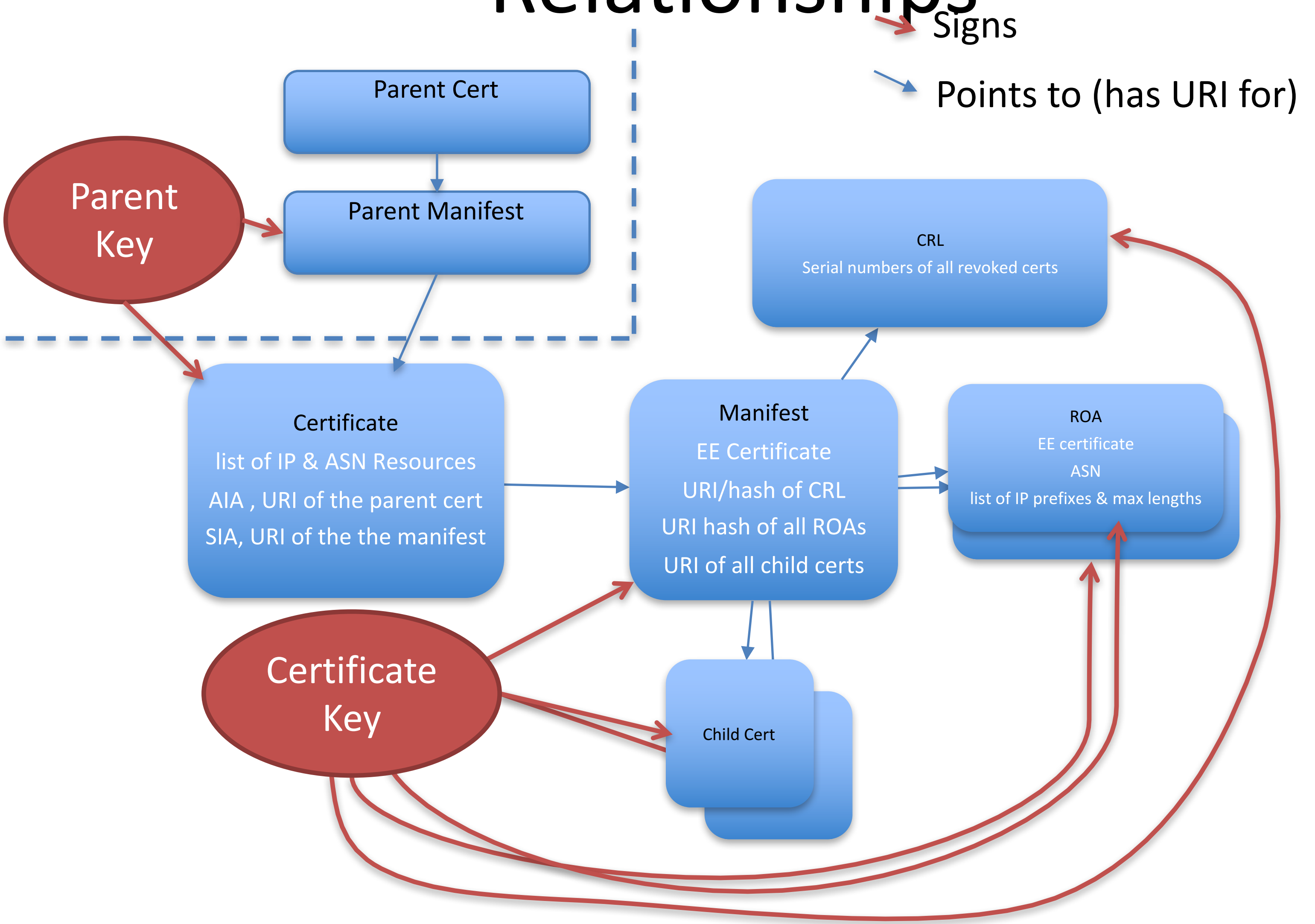
Other Small ISP
192.78.12.0/24

192.78.12.0/24
AS2000

What does RPKI Create?

- **It creates a repository**
  - RFC 3779 (RPKI) Certificates
  - ROAs
  - CRLs
  - Manifest records

Relationships



Signs

Points to (has URI for)

Parent Cert

Parent Key

Parent Manifest

CRL
Serial numbers of all revoked certs

Certificate
list of IP & ASN Resources
AIA , URI of the parent cert
SIA, URI of the the manifest

Manifest
EE Certificate
URI/hash of CRL
URI hash of all ROAs
URI of all child certs

ROA
EE certificate
ASN
list of IP prefixes & max lengths

Certificate Key

Child Cert

Repository View

```
./ba/03a5be-ddf6-4340-a1f9-1ad3f2c39ee6/1:
total 40
-rw-r--r--  1 143  143  1543 Jun 26  2009 ICcaIRKhGHJ-TgUZv8GRKqkidR4.roa
-rw-r--r--  1 143  143  1403 Jun 26  2009 cKxLCU94umS-qD4DOOkAK0M2US0.cer
-rw-r--r--  1 143  143  485  Jun 26  2009 dSmerM6uJGLWMMQTl2esy4xyUAA.crl
-rw-r--r--  1 143  143  1882 Jun 26  2009 dSmerM6uJGLWMMQTl2esy4xyUAA.mnf
-rw-r--r--  1 143  143  1542 Jun 26  2009 nB0gDFtWffKk4VWgln-12pdFtE8.roa
```

A Repository Directory containing an RFC3779 Certificate, two ROAs, a CRL, and a manifest

Repository Use

- Pull down these files using a manifest-validating mechanism
- Validate the ROAs contained in the repository
- Communicate with the router marking routes "valid", "invalid", "unknown"
- Up to ISP to use local policy on how to route

Possible Data Flow for Operations

- RPKI Web interface -> Repository
- Repository aggregator -> Validator
- Validated entries -> Route Checking
- Route checking results -> local routing decisions (based on local policy)

How you can use ARIN’s RPKI System?

- Hosted
  - create ROAs through ARIN Online
  - create ROAs using ARIN’s RESTful service
- Delegated using Up/Down Protocol

Hosted RPKI - ARIN Online

- **Pros**
  - – Easy to pick up and use
  - – ARIN managed
- **Cons**
  - – No current support for downstream customers to manage their own space
  - – Tedious through the UI if you have a large network
  - – We hold your private key

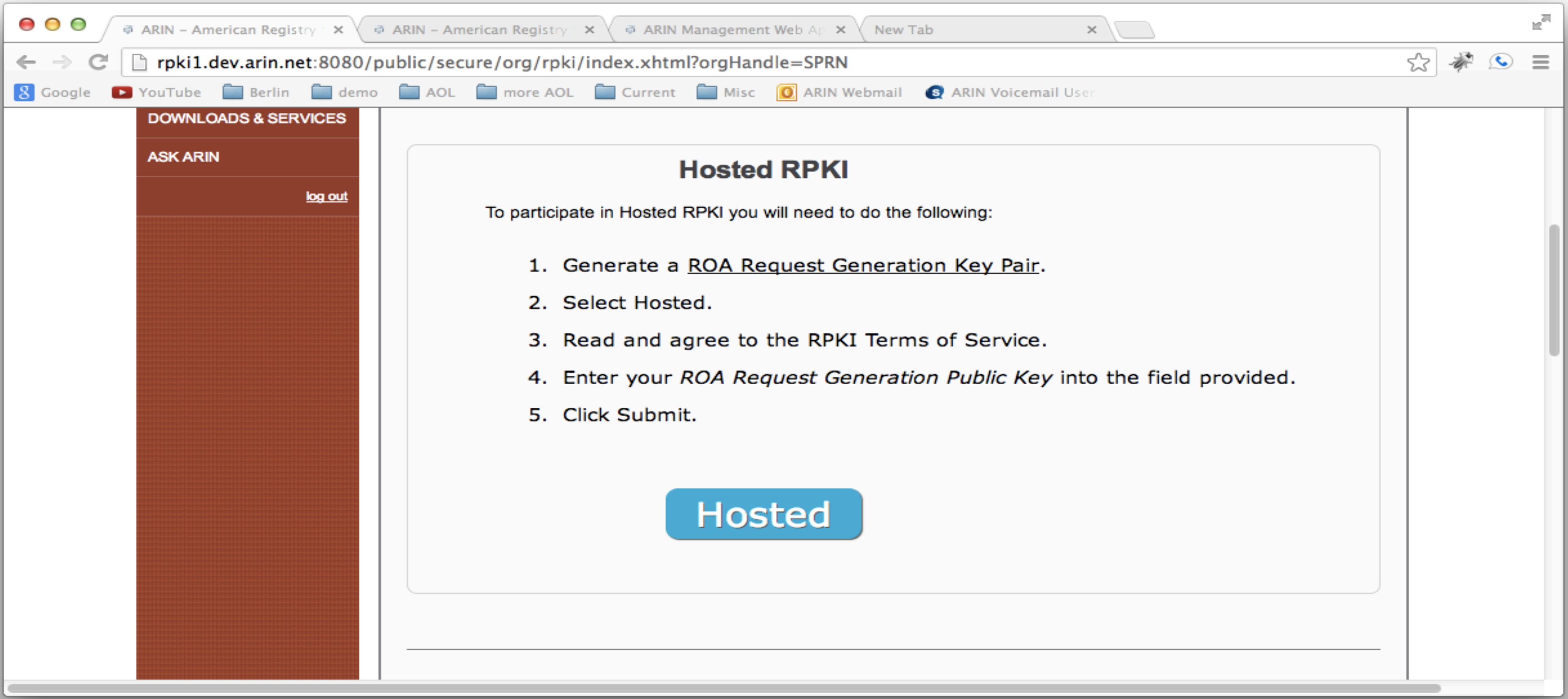
Hosted RPKI - RESTful Interace

- **Pros**
  - – Programmatic interface for large networks
  - – ARIN managed
- **Cons**
  - – No current support for downstream customers to manage their own space
  - – We hold your private key

Delegated RPKI with Up/Down

- **Pros**
  - You safeguard your own private key
  - Follows the IETF up/down protocol
- **Cons**
  - Extremely hard to setup
  - Need to operate your own RPKI environment

Hosted RPKI in ARIN Online

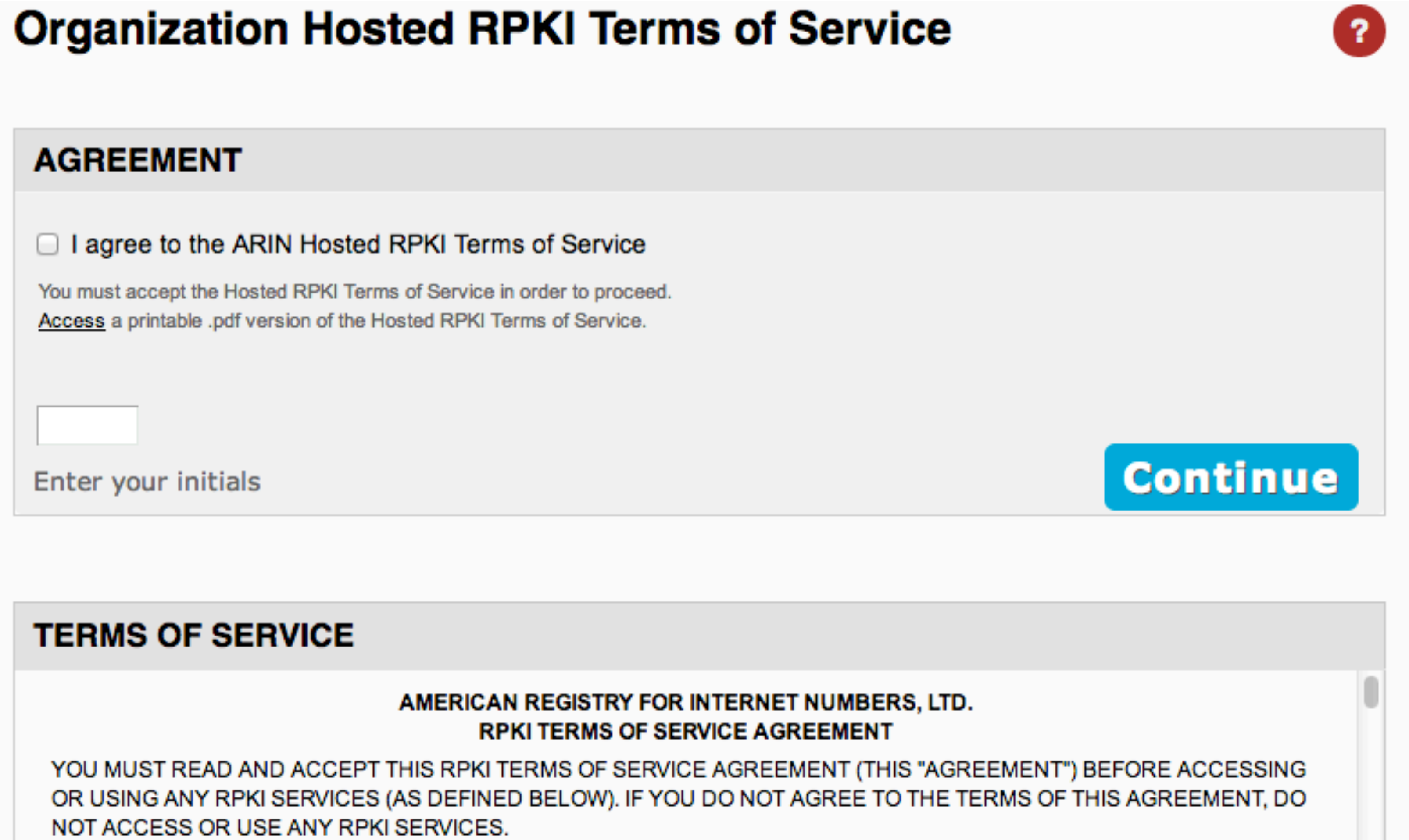


Hosted RPKI

To participate in Hosted RPKI you will need to do the following:

1. Generate a ROA Request Generation Key Pair.
2. Select Hosted.
3. Read and agree to the RPKI Terms of Service.
4. Enter your *ROA Request Generation Public Key* into the field provided.
5. Click Submit.

Hosted RPKI in ARIN Online



Organization Hosted RPKI Terms of Service

AGREEMENT

☐ I agree to the ARIN Hosted RPKI Terms of Service

You must accept the Hosted RPKI Terms of Service in order to proceed.
Access a printable .pdf version of the Hosted RPKI Terms of Service.

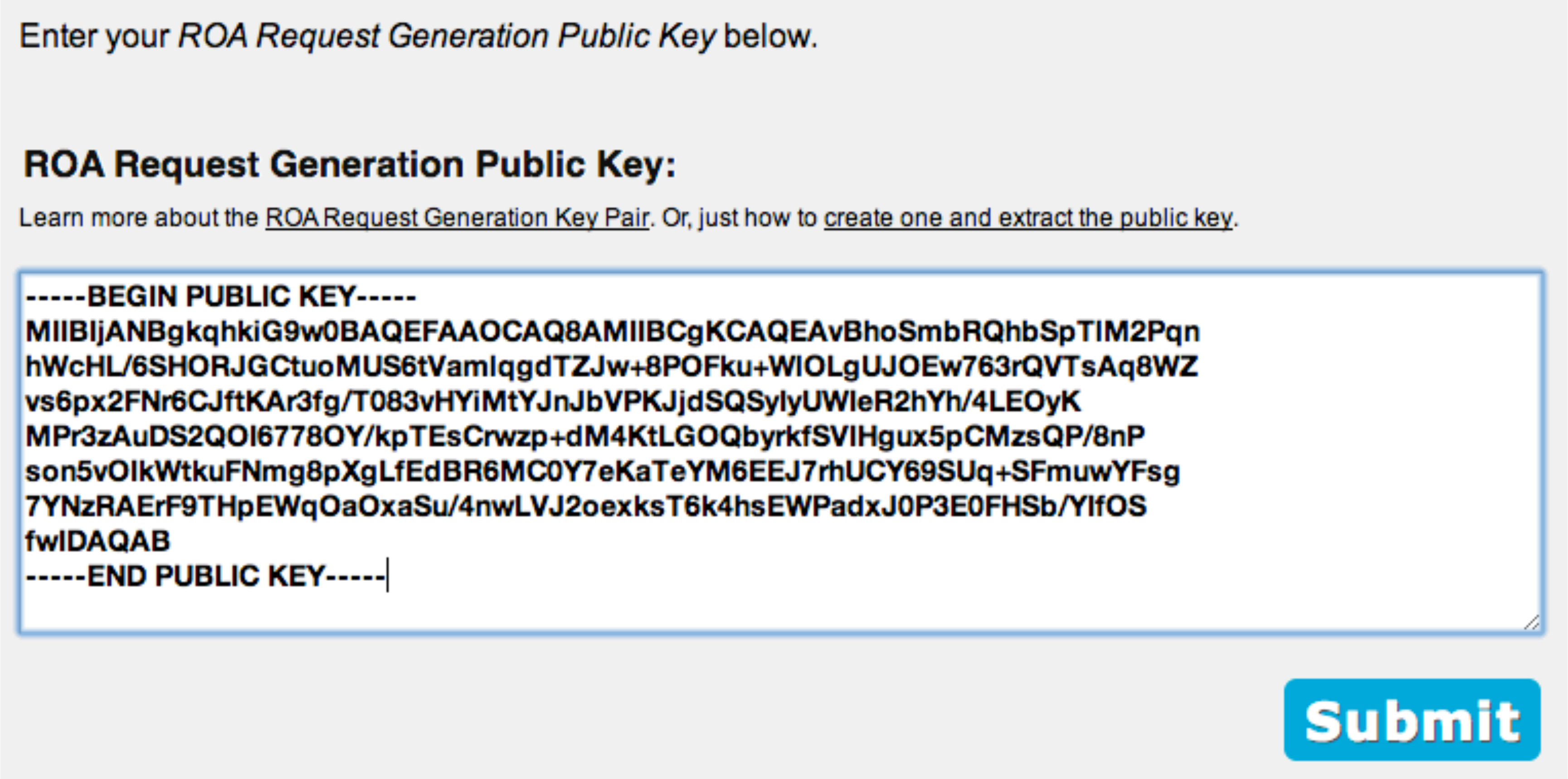
Enter your initials

TERMS OF SERVICE

AMERICAN REGISTRY FOR INTERNET NUMBERS, LTD.
RPKI TERMS OF SERVICE AGREEMENT

YOU MUST READ AND ACCEPT THIS RPKI TERMS OF SERVICE AGREEMENT (THIS "AGREEMENT") BEFORE ACCESSING OR USING ANY RPKI SERVICES (AS DEFINED BELOW). IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT ACCESS OR USE ANY RPKI SERVICES.

Hosted RPKI in ARIN Online



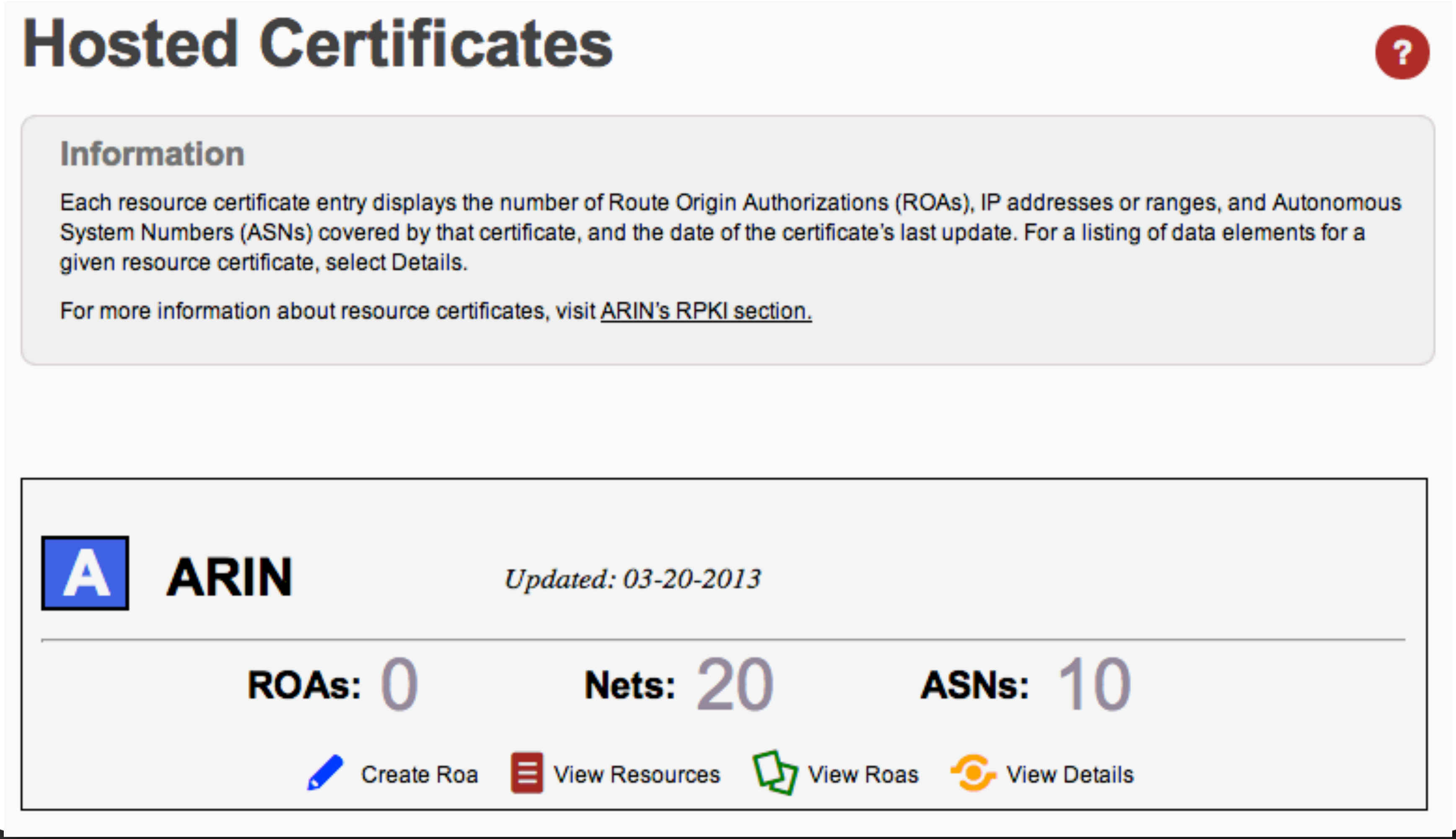
Enter your *ROA Request Generation Public Key* below.

ROA Request Generation Public Key:

Learn more about the ROA Request Generation Key Pair. Or, just how to create one and extract the public key.

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvBhoSmbRQhbSpTIM2Pqn
hWcHL/6SHORJGCtuoMUS6tVamIqgdTZJw+8POFku+WIOLgUJOEw763rQVTsAq8WZ
vs6px2FNr6CJftKAr3fg/T083vHYiMtYJnJbVPKJjdSQSylyUWIeR2hYh/4LEOyK
MPr3zAuDS2QOI6778OY/kpTEsCrwzp+dM4KtLGOQbyrkfSVIHgux5pCMzsQP/8nP
son5vOIkWtkuFNmg8pXgLfEdBR6MC0Y7eKaTeYM6EEJ7rhUCY69SUq+SFmuwYFsg
7YNzRAErF9THpEWqOaOxaSu/4nwLVJ2oexksT6k4hsEWPadxJ0P3E0FHSb/YIfOS
fwIDAQAB
-----END PUBLIC KEY-----
```

Hosted RPKI in ARIN Online



Hosted Certificates

Information

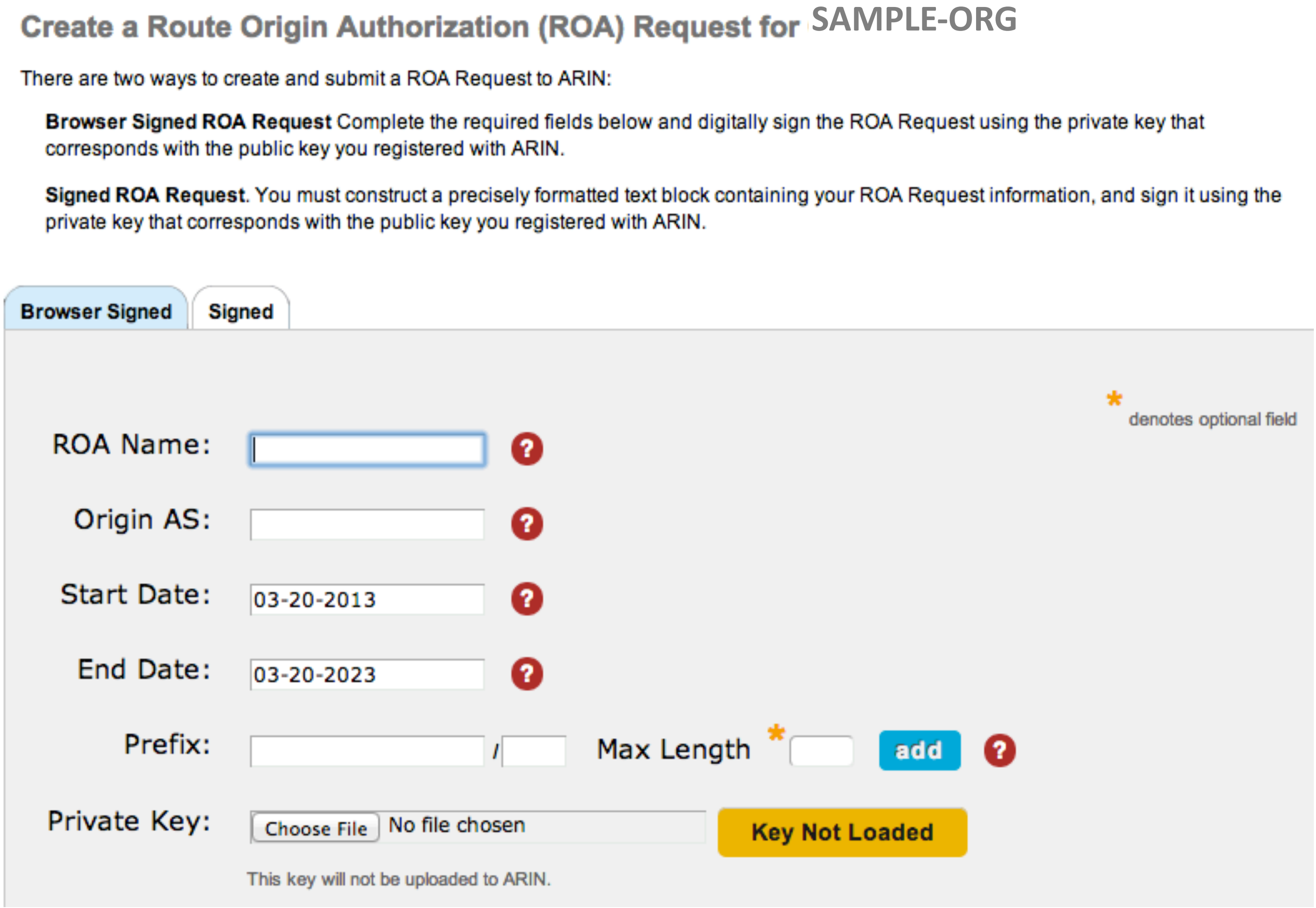
Each resource certificate entry displays the number of Route Origin Authorizations (ROAs), IP addresses or ranges, and Autonomous System Numbers (ASNs) covered by that certificate, and the date of the certificate's last update. For a listing of data elements for a given resource certificate, select Details.

For more information about resource certificates, visit ARIN's RPKI section.

A ARIN *Updated: 03-20-2013*

ROAs: 0 **Nets:** 20 **ASNs:** 10

Hosted RPKI in ARIN Online



Create a Route Origin Authorization (ROA) Request for SAMPLE-ORG

There are two ways to create and submit a ROA Request to ARIN:

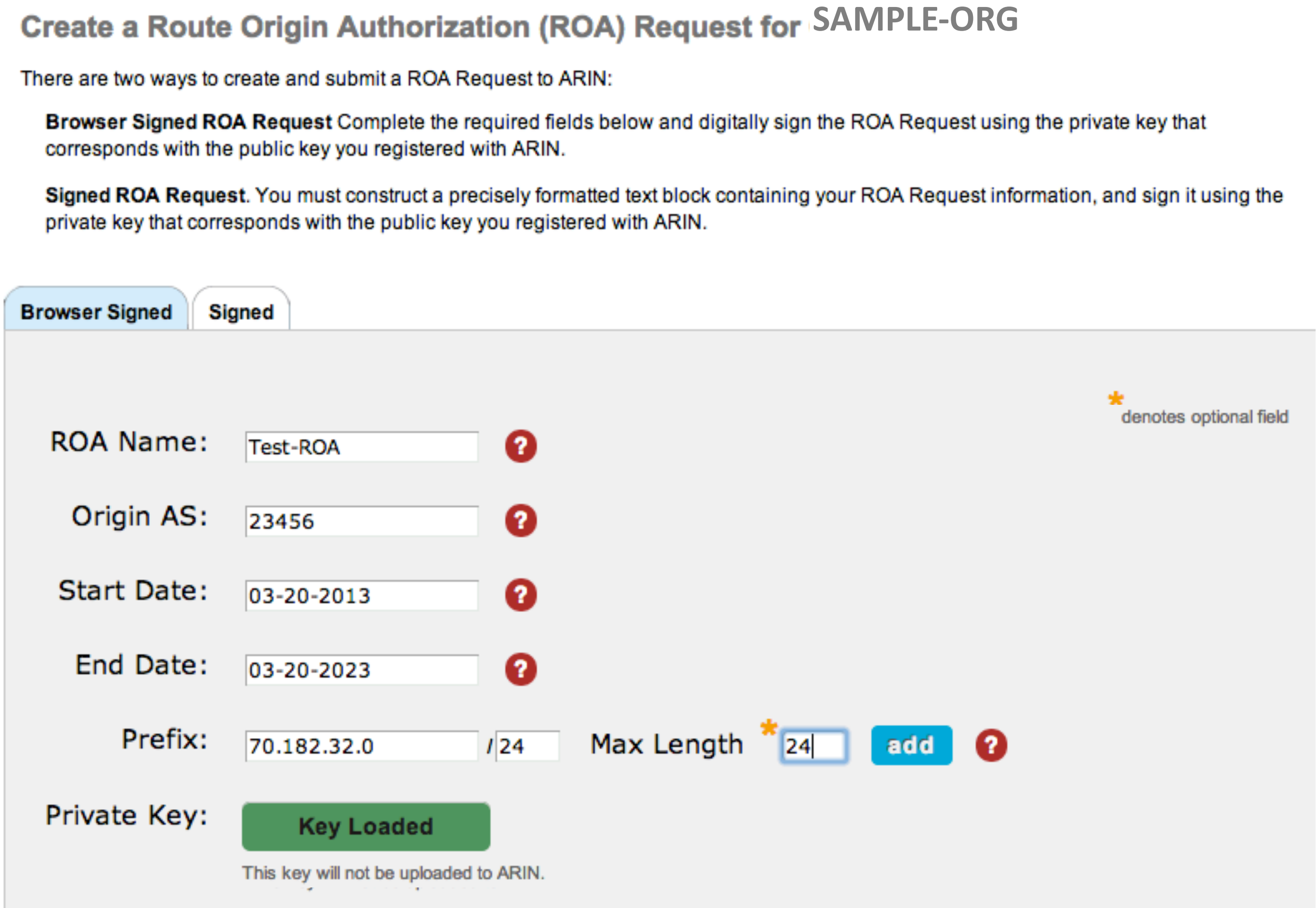
Browser Signed ROA Request Complete the required fields below and digitally sign the ROA Request using the private key that corresponds with the public key you registered with ARIN.

Signed ROA Request. You must construct a precisely formatted text block containing your ROA Request information, and sign it using the private key that corresponds with the public key you registered with ARIN.

ROA Name:	
Origin AS:	
Start Date:	03-20-2013
End Date:	03-20-2023
Prefix:	/ Max Length *
Private Key:	No file chosen

This key will not be uploaded to ARIN.

Hosted RPKI in ARIN Online



Create a Route Origin Authorization (ROA) Request for SAMPLE-ORG

There are two ways to create and submit a ROA Request to ARIN:

Browser Signed ROA Request Complete the required fields below and digitally sign the ROA Request using the private key that corresponds with the public key you registered with ARIN.

Signed ROA Request. You must construct a precisely formatted text block containing your ROA Request information, and sign it using the private key that corresponds with the public key you registered with ARIN.

ROA Name: Test-ROA

Origin AS: 23456

Start Date: 03-20-2013

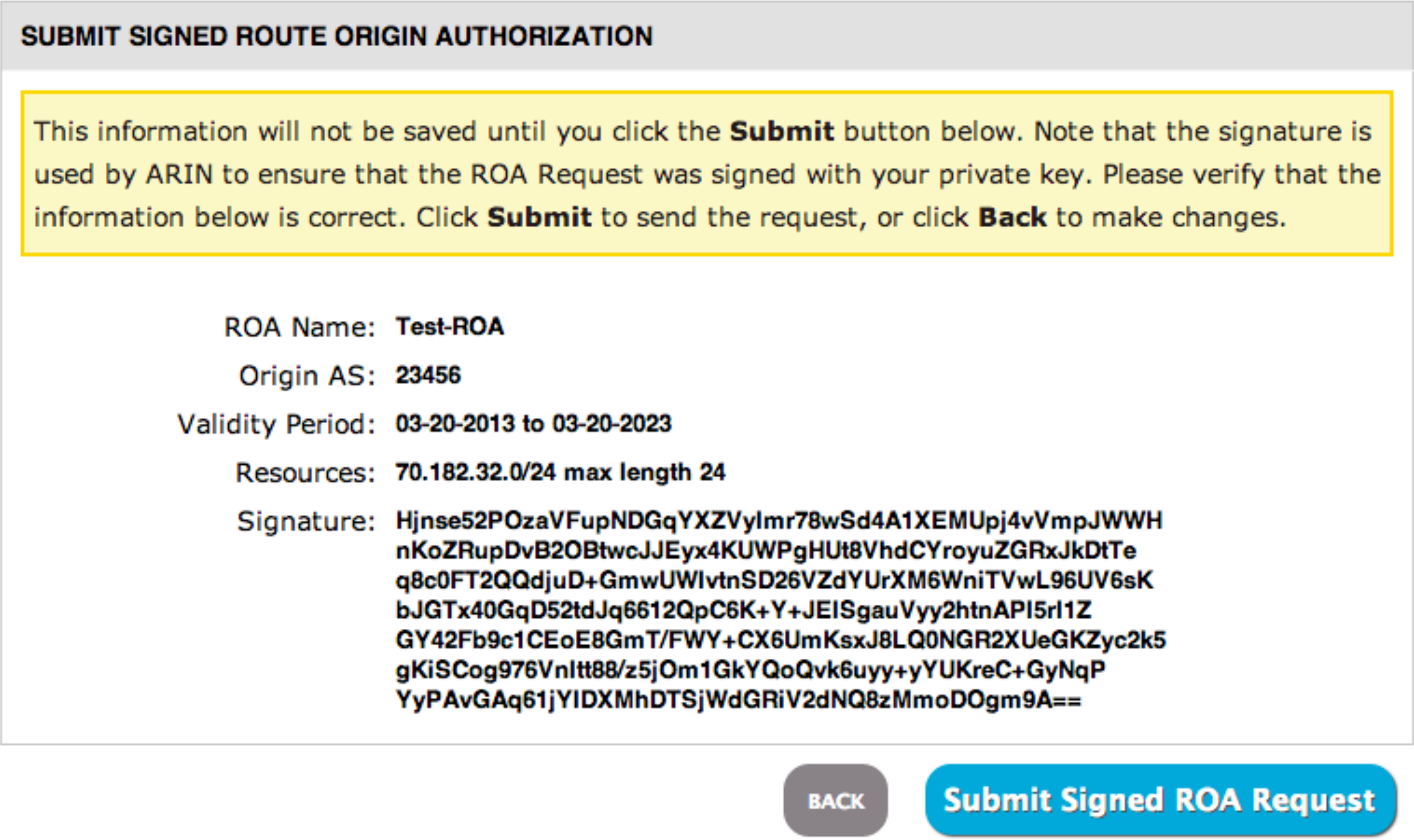
End Date: 03-20-2023

Prefix: 70.182.32.0 / 24 Max Length * 24

Private Key: Key Loaded

This key will not be uploaded to ARIN.

Hosted RPKI in ARIN Online



SUBMIT SIGNED ROUTE ORIGIN AUTHORIZATION

This information will not be saved until you click the **Submit** button below. Note that the signature is used by ARIN to ensure that the ROA Request was signed with your private key. Please verify that the information below is correct. Click **Submit** to send the request, or click **Back** to make changes.

ROA Name: **Test-ROA**

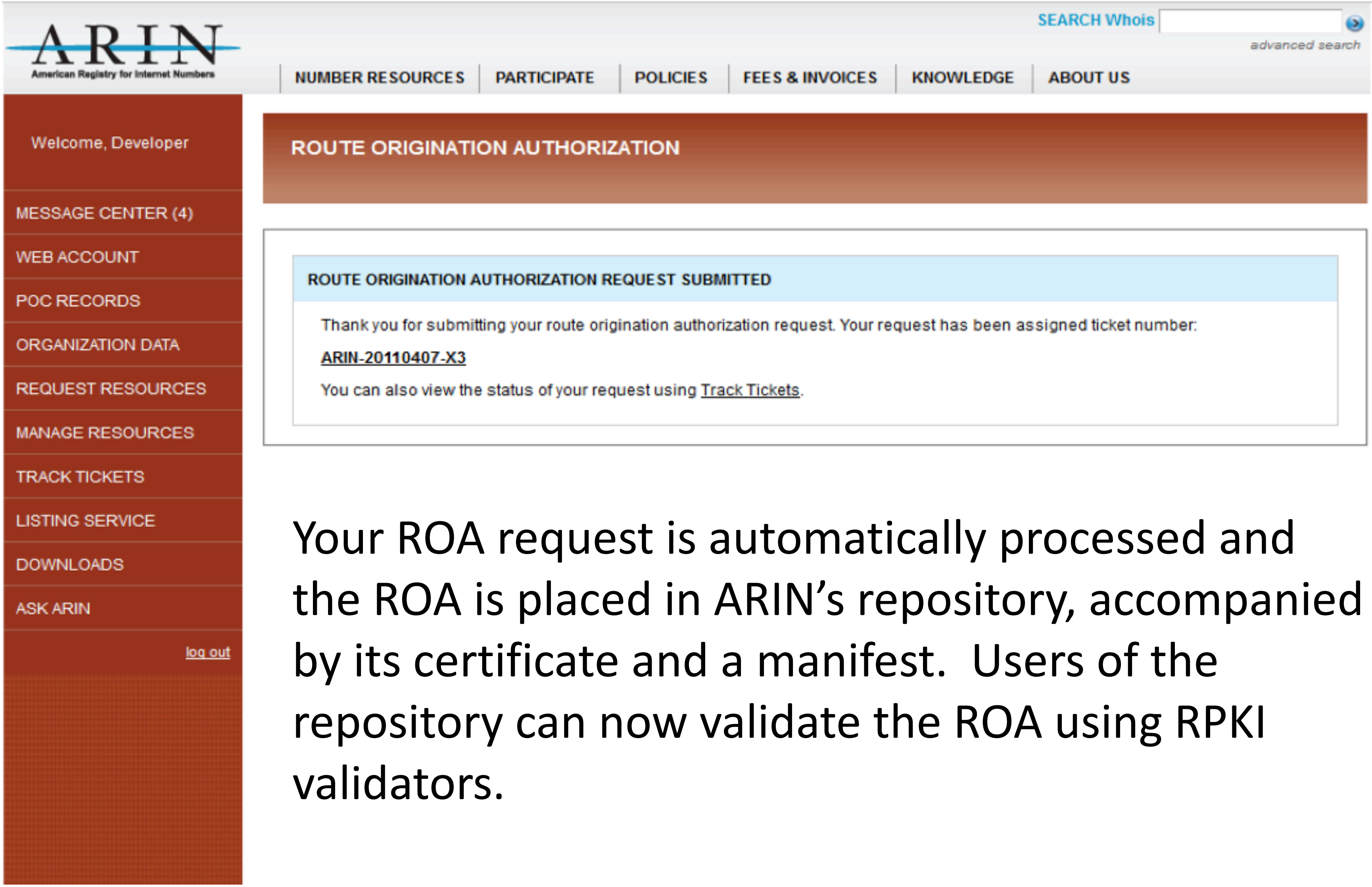
Origin AS: **23456**

Validity Period: **03-20-2013 to 03-20-2023**

Resources: **70.182.32.0/24 max length 24**

Signature:

Hjnse52POzaVFupNDGqYXZVylmr78wSd4A1XEMUpj4vVmpJWWH
nKoZRupDvB2OBtwcJJEyx4KUWPgHUt8VhdCYroyuZGRxJkDtTe
q8c0FT2QQdjuD+GmwUWlvtnSD26VZdYUrXM6WniTVwL96UV6sK
bJGTx40GqD52tdJq6612QpC6K+Y+JEISgauVyy2htnAPI5rl1Z
GY42Fb9c1CEoE8GmT/FWY+CX6UmKsxJ8LQ0NGR2XUeGKZyc2k5
gKiSCog976VnItt88/z5jOm1GkYQoQvk6uyy+yYUKreC+GyNqP
YyPAvGAq61jYIDXMhDTSjWdGRiV2dNQ8zMmoDOgm9A==



ROUTE ORIGINATION AUTHORIZATION

ROUTE ORIGINATION AUTHORIZATION REQUEST SUBMITTED

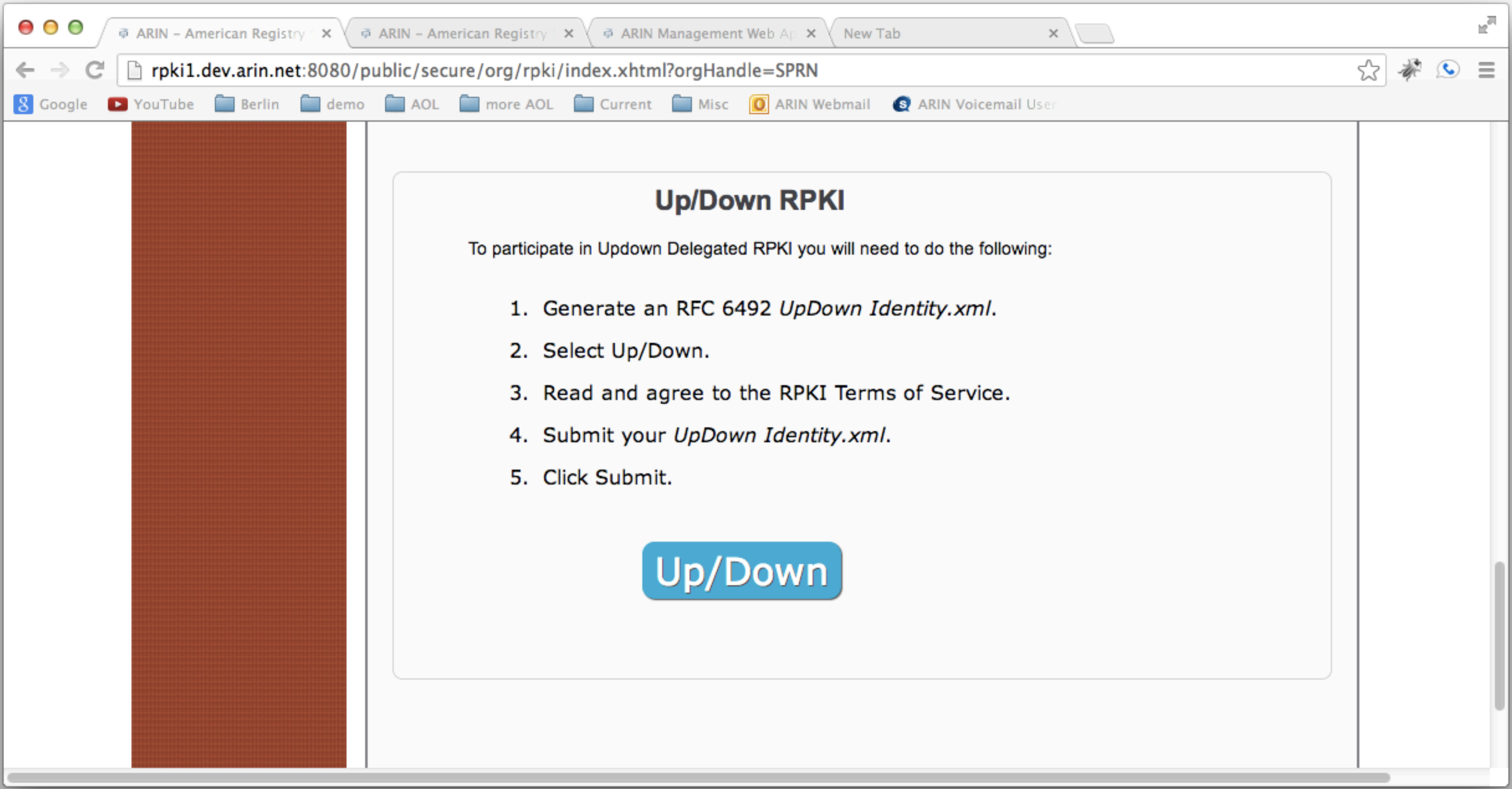
Thank you for submitting your route origination authorization request. Your request has been assigned ticket number:

ARIN-20110407-X3

You can also view the status of your request using Track Tickets.

Your ROA request is automatically processed and the ROA is placed in ARIN’s repository, accompanied by its certificate and a manifest. Users of the repository can now validate the ROA using RPKI validators.

Delegated with Up/Down

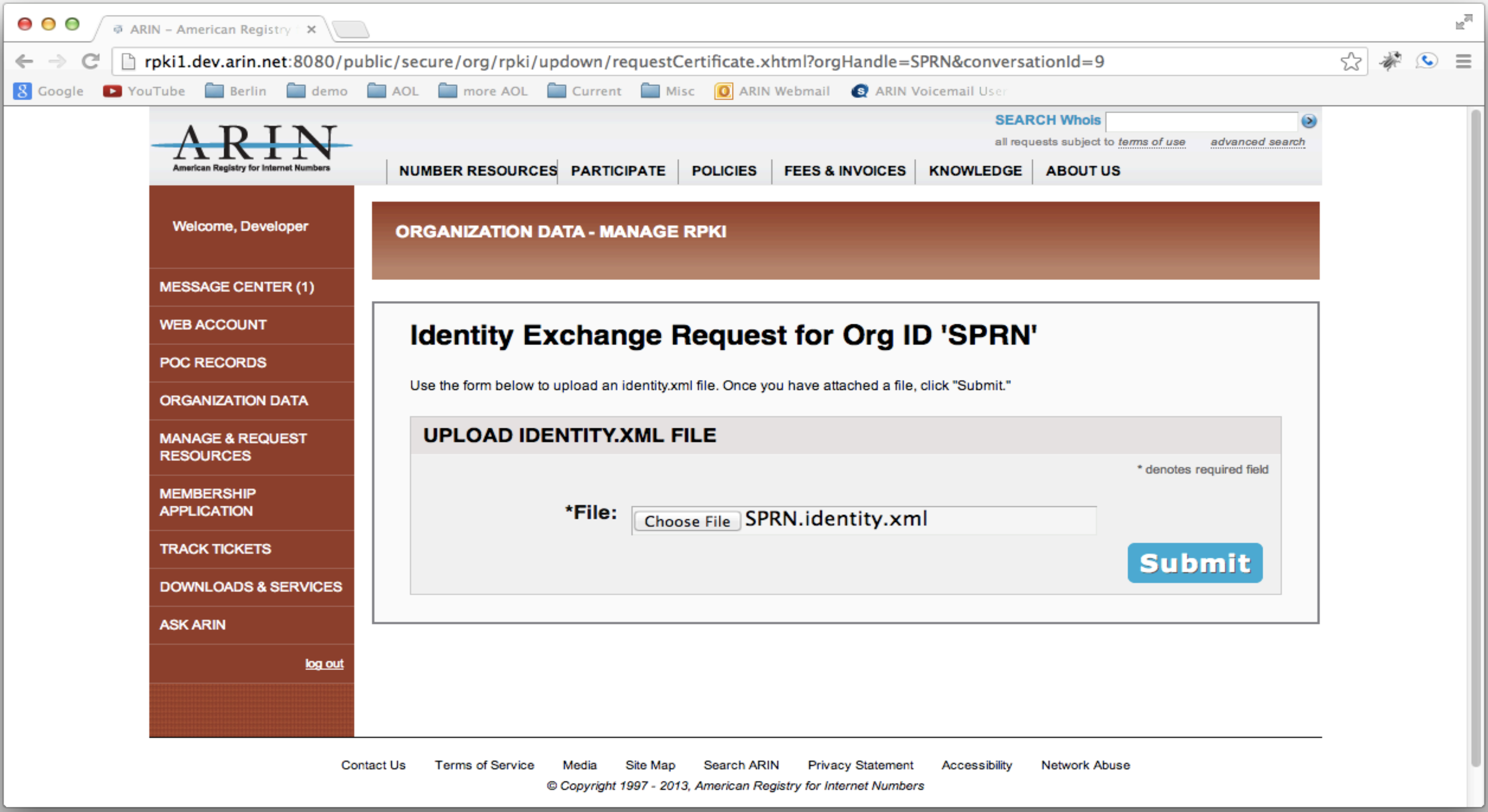


Up/Down RPKI

To participate in Updown Delegated RPKI you will need to do the following:

1. Generate an RFC 6492 *UpDown Identity.xml*.
2. Select Up/Down.
3. Read and agree to the RPKI Terms of Service.
4. Submit your *UpDown Identity.xml*.
5. Click Submit.

Delegated with Up/Down



ORGANIZATION DATA - MANAGE RPKI

Identity Exchange Request for Org ID 'SPRN'

Use the form below to upload an identity.xml file. Once you have attached a file, click "Submit."

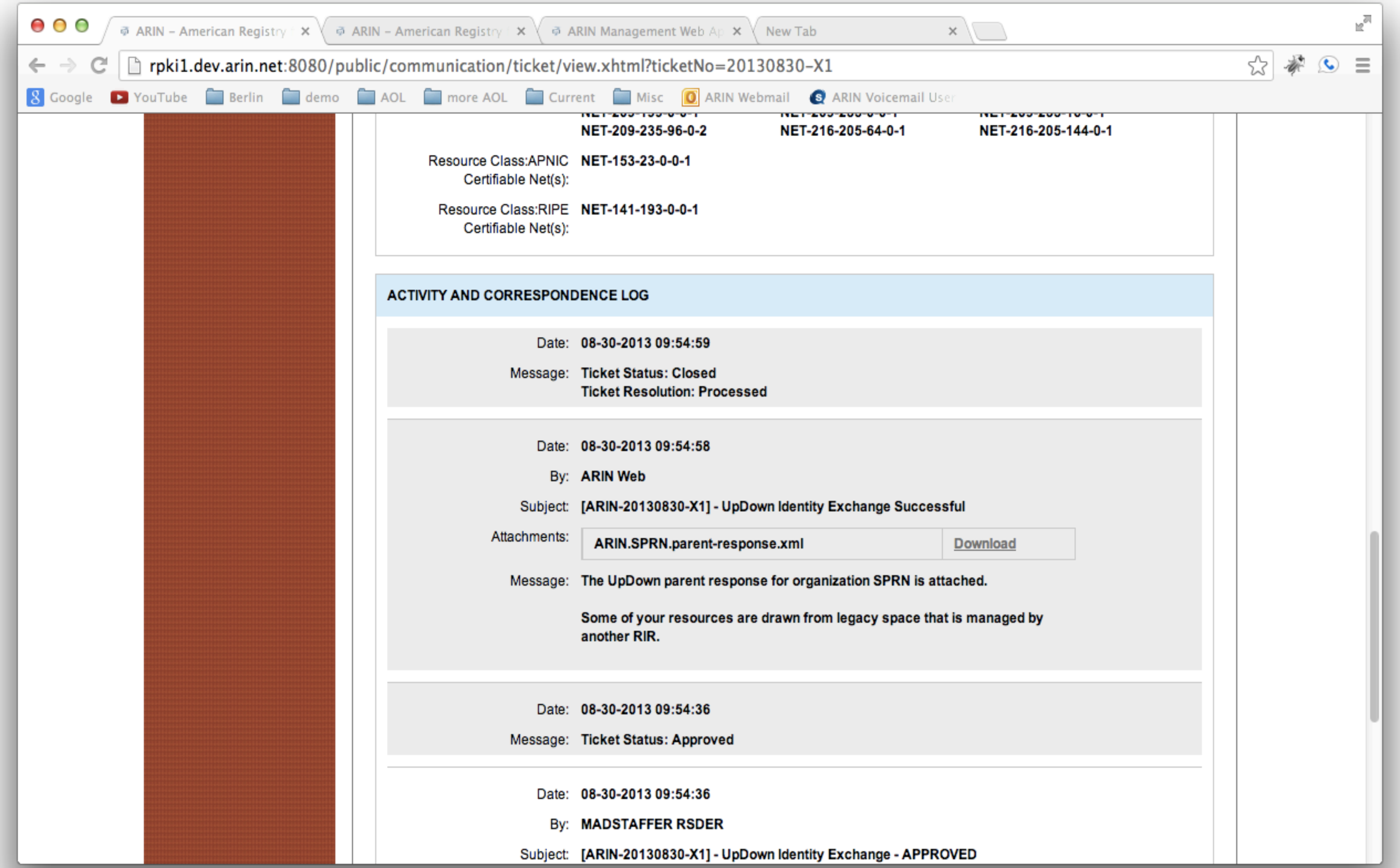
UPLOAD IDENTITY.XML FILE

* denotes required field

*File: Choose File SPRN.identity.xml

© Copyright 1997 - 2013, American Registry for Internet Numbers

Delegated with Up/Down



NET-209-235-96-0-2 NET-216-205-64-0-1 NET-216-205-144-0-1

Resource Class:APNIC Certifiable Net(s): NET-153-23-0-0-1

Resource Class:RIPE Certifiable Net(s): NET-141-193-0-0-1

ACTIVITY AND CORRESPONDENCE LOG

Date: 08-30-2013 09:54:59

Message: Ticket Status: Closed
Ticket Resolution: Processed

Date: 08-30-2013 09:54:58

By: ARIN Web

Subject: [ARIN-20130830-X1] - UpDown Identity Exchange Successful

Attachments: ARIN.SPRN.parent-response.xml Download

Message: The UpDown parent response for organization SPRN is attached.

Some of your resources are drawn from legacy space that is managed by another RIR.

Date: 08-30-2013 09:54:36

Message: Ticket Status: Approved

Date: 08-30-2013 09:54:36

By: MADSTAFFER RSDER

Subject: [ARIN-20130830-X1] - UpDown Identity Exchange - APPROVED

Delegated with Up/Down

- You have to do all the ROA creation
- Need to setup a Certificate Authority
- Have a highly available repository
- Create a CPS

RPKI Statistics

	Apr 2013	Oct 2013	Apr 2014	Oct 2014	Apr 2015	Oct 2015	Apr 2016	Sep 2016
Certified Orgs	47	68	108	153	187	220	250	263
ROAs	60	106	162	239	308	338	370	410
Covered Resources	82	147	258	332	430	482	528	582
Up/Down Delegated		0	0	0	1	2	1	2

Q&A