



American Registry for Internet Numbers

Security Overlays on Core Internet Protocols – DNSSEC and RPKI

Mark Kosters

ARIN CTO

Why are DNSSEC and RPKI Important

- Two critical resources
 - DNS
 - Routing
- Hard to tell if compromised
 - From the user point of view
 - From the ISP/Enterprise
- Focus on government funding

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

- Only key holders may create and submit Delegation Signer (DS) records
- DNSSEC users need to 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
<input checked="" type="checkbox"/>	252.149.192.in-addr.arpa.	NS1.ARIN.NET NS2.ARIN.NET NS2.LACNIC.NET SEC1.APNIC.NET SEC1.AUTHDNS.RIPE.NET		ARIN Operations

[MODIFY NAMESERVERS](#)

[MODIFY DS RECORDS](#)

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:

Nameserver 2:

Nameserver 3:

Nameserver 4:

Nameserver 5:

Nameserver 6:

Nameserver 13:

APPLY TO ALL

CANCEL

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

[Parse DS Record](#)

Choose File No file chosen

UPLOAD FILE

File contents must be plain text

APPLY TO ALL

CANCEL

Reverse DNS: Querying ARIN's Whois

Query for the zone directly:

```
whois> 81.147.204.in-addr.arpa
```

```
Name:                81.147.204.in-addr.arpa.  
Updated:             2006-05-15  
NameServer:          AUTHNS2.DNVR.QWEST.NET  
NameServer:          AUTHNS3.STTL.QWEST.NET  
NameServer:          AUTHNS1.MPLS.QWEST.NET
```

```
Ref:    http://whois.arin.net/rest/rdns/81.147.204.in-addr.arpa.
```

DNSSEC in Zone Files

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+sbzQN4LmHzl0i0C/hkaSV03q1y
                        6J0KjqNPzYqtxLgZjU+IL9qhtIOocgNQib9l
                        gFRmZ9inf2bER435GMsa/nnjpVVWW/MBRKxf
                        Pcc72w2i0AMu2G0prtVT08ENxtu/pBfns0ZK
                        nhCY8U0BOYLOLE5Whtk3X0uX9+U= )
NSEC                    10800 NSEC 1.121.74.in-addr.arpa. NS DS RRSIG
                        10800 RRSIG NSEC 5 5 10800 20140306210053 (
                        20140224210053 57974 74.in-addr.arpa.
                        YvRowkdVDfv+PW42ySNUwW8S8jRyV6EKKRxe
```

...

DNSSEC

Oct 2015	
Number of Orgs with DNSSEC	123
Total Number of Delegations	583,442
DNSSEC Secured Zones	586
Percentage Secured	0.1 %

DNSSEC Validating Resolvers

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

Reverse DNS Management and DNSSEC in ARIN Online

- Available on ARIN's website

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



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

Resource Cert Validation

Resource
Allocation
Hierarchy

AFRINIC

RIPE NCC

APNIC

ICANN

ARIN

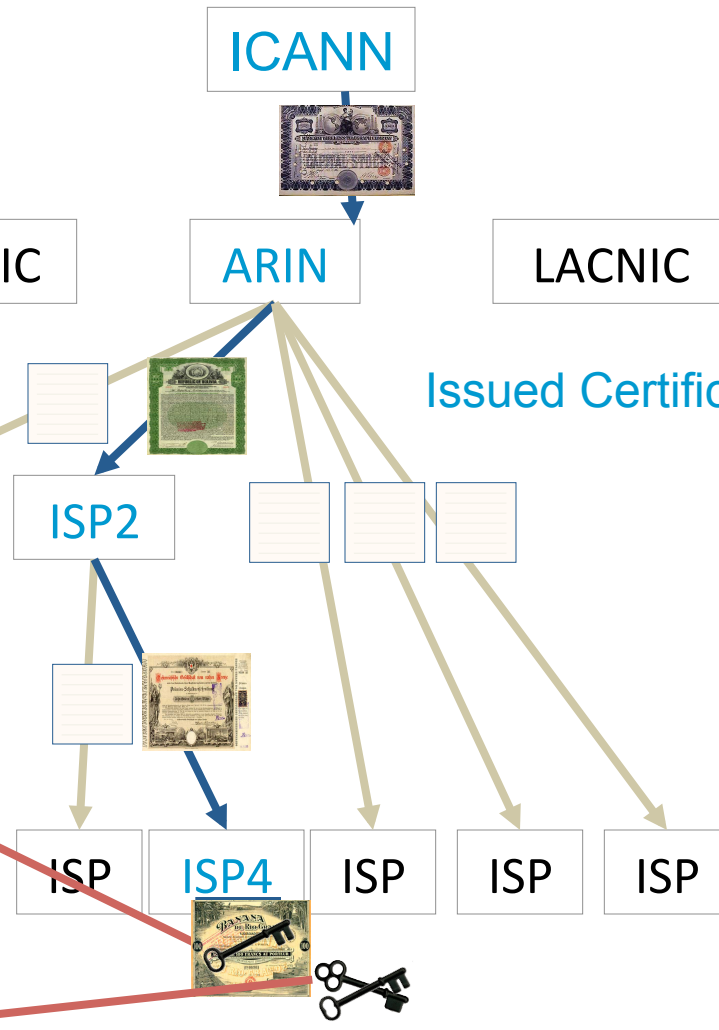
LACNIC

Issued Certificates

Route Origination Authority
"ISP4 permits AS65000 to
originate a route for the
prefix 192.2.200.0/24"

Attachment: <isp4-ee-cert>

Signed,
ISP4 <isp4-ee-key-priv>



Resource Cert Validation

Resource
Allocation
Hierarchy



ICANN



ARIN

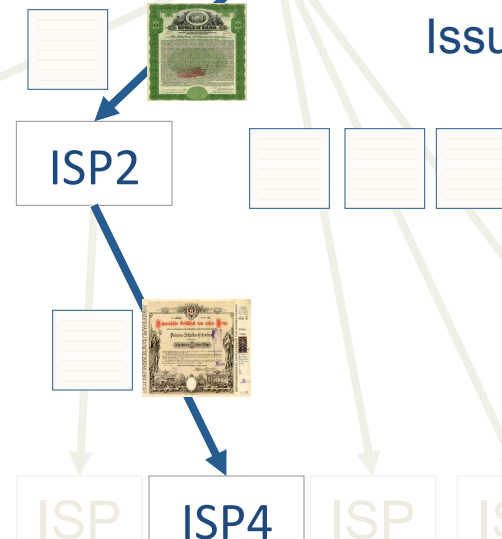
LACNIC

Issued Certificates

Route Origination Authority
"ISP4 permits AS65000 to
originate a route for the
prefix 192.2.200.0/24"

Attachment: <isp4-ee-cert>

Signed,
ISP4 <isp4-ee-key-priv>



1. Did the matching private key
sign this text?

Resource Cert Validation

Resource
Allocation
Hierarchy



ICANN



ARIN

LACNIC

Issued Certificates

Route Origination Authority
"ISP4 permits AS65000 to
originate a route for the
prefix 192.2.200.0/24"

Attachment: **<isp4-ee-cert>**

Signed,
ISP4 **<isp4-ee-key-priv>**

ISP2



ISP

ISP4

ISP

ISP

ISP



2. Is this certificate valid?

Resource Cert Validation

Resource
Allocation
Hierarchy



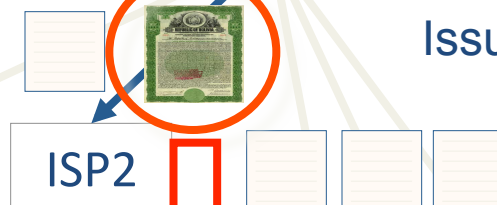
ICANN



AN

LACNIC

Issued Certificates



Route Origination Authority
"ISP4 permits AS65000 to originate a route for the prefix 192.2.200.0/24"

Attachment: **<isp4-ee-cert>**

Signed,
ISP4 **<isp4-ee-key-priv>**



3. Is there a valid certificate path from a Trust Anchor to this certificate?

What does RPKI Create?

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

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
- Hosted using ARIN's RESTful service
- Delegated using Up/Down Protocol

Hosted RPKI

- Pros
 - Easier to use
 - ARIN managed
- Cons
 - No current support for downstream customers to manage their own space (yet)
 - Tedious through the IU if you have a large network
 - We hold your private key

Hosted RPKI with RESTful Interface

- Pros
 - Easier to use
 - ARIN managed
 - Programmatic interface for large networks
- Cons
 - No current support for downstream customers to manage their own space (yet)
 - We hold your private key

Delegated RPKI with Up/Down

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

Hosted RPKI in ARIN Online

The screenshot shows a web browser window with the ARIN Management Web App. The address bar displays the URL `rpki1.dev.arin.net:8080/public/secure/org/rpki/index.xhtml?orgHandle=SPRN`. The browser's address bar also shows several bookmarks: Google, YouTube, Berlin, demo, AOL, more AOL, Current, Misc, ARIN Webmail, and ARIN Voicemail User. The page layout includes a left sidebar with a red header containing the text "DOWNLOADS & SERVICES" and "ASK ARIN", and a "log out" link. The main content area is titled "Hosted RPKI" and contains the following text: "To participate in Hosted RPKI you will need to do the following:". Below this text is a numbered list of five steps: 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. At the bottom of the main content area is a blue button labeled "Hosted".

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

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

Continue

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-----

```
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA vBhoSmbRQhbSpTIM2Pqn  
hWcHL/6SHORJGctuoMUS6tVamlqgdTZJw+8POFku+WIOlgUJOEw763rQVTsAq8WZ  
vs6px2FNr6CJftKAr3fg/T083vHYIMtYJnJbVPKJjdSQSylyUWleR2hYh/4LEOyK  
MPr3zAuDS2QOI6778OY/kpTEsCrwzp+dM4KtLGOQbyrkfSVIHgux5pCMzsQP/8nP  
son5vOIkWtkuFNmg8pXgLfEdBR6MC0Y7eKaTeYM6EEJ7rhUCY69SUq+SFmuwYFsg  
7YNzRAErF9THpEWqOaOxaSu/4nwLVJ2oexksT6k4hsEWPadxJ0P3E0FHSb/YIfOS  
fwIDAQAB
```

-----END PUBLIC KEY-----|

Submit

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](#).



ARIN

Updated: 03-20-2013

ROAs: 0

Nets: 20

ASNs: 10



Create Roa



View Resources



View Roas



View Details

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.

Browser Signed**Signed**


 denotes optional field

ROA Name: ?

Origin AS: ?

Start Date: ?

End Date: ?

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.

Browser Signed**Signed**

denotes optional field

ROA Name: ?

Origin AS: ?

Start Date: ?

End Date: ?

Prefix: / Max Length ?

Private Key:

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+JEISgauVyy2htnAPI5r1Z
GY42Fb9c1CEoE8GmT/FWY+CX6UmKsxJ8LQ0NGR2XUeGKZyc2k5
gKiSCog976Vnltt88/z5jOm1GkYQoQvk6uyy+yYUKreC+GyNqP
YyPAvGAq61jYIDXMhDTSjWdGRiV2dNQ8zMmoDOgm9A==**

BACK

Submit Signed ROA Request

ARIN
American Registry for Internet Numbers

SEARCH Whois [advanced search](#)

NUMBER RESOURCES PARTICIPATE POLICIES FEES & INVOICES KNOWLEDGE ABOUT US

Welcome, Developer

MESSAGE CENTER (4)

WEB ACCOUNT

POC RECORDS

ORGANIZATION DATA

REQUEST RESOURCES

MANAGE RESOURCES

TRACK TICKETS

LISTING SERVICE

DOWNLOADS

ASK ARIN

[log out](#)

ROUTE ORIGATION AUTHORIZATION

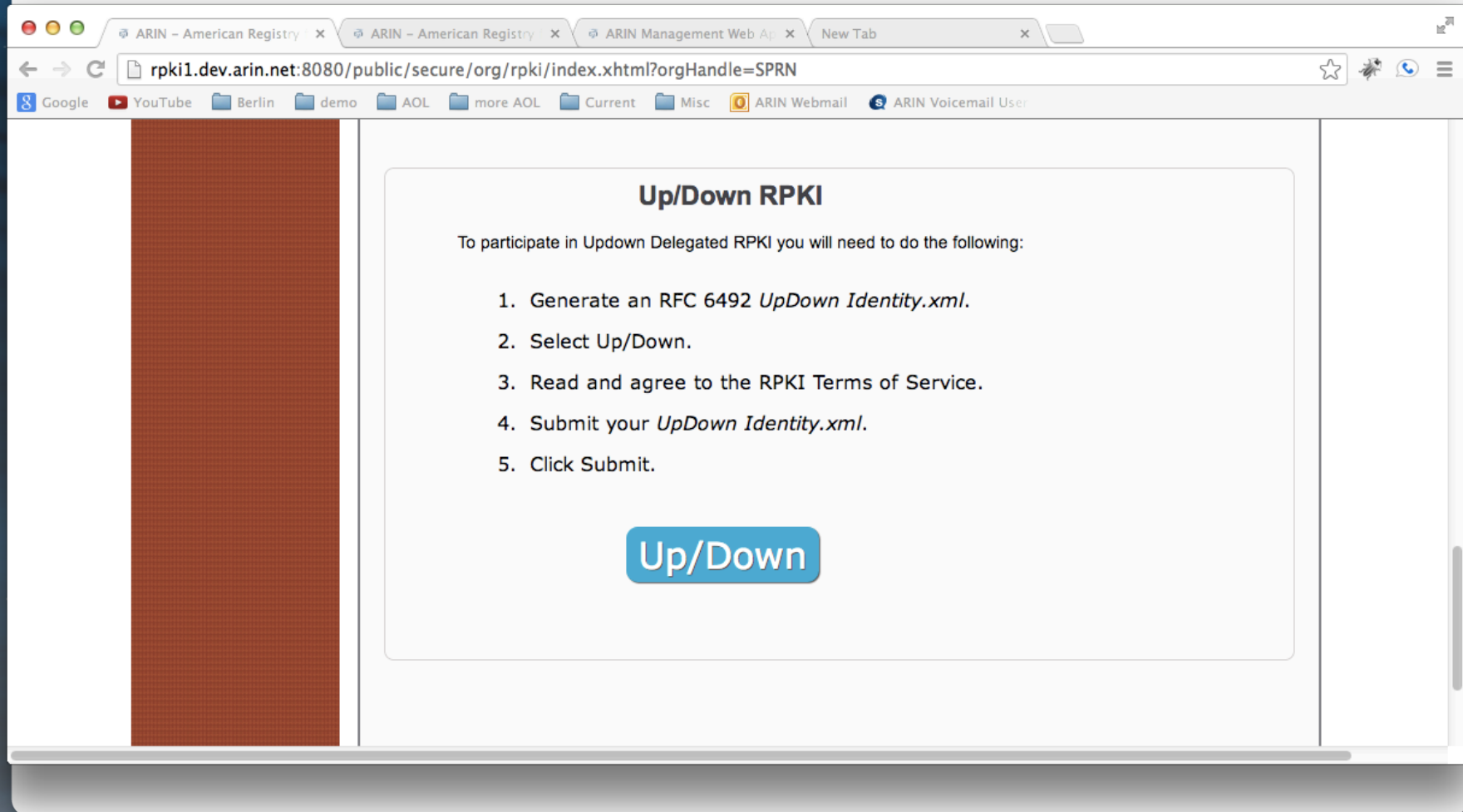
ROUTE ORIGATION AUTHORIZATION REQUEST SUBMITTED

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



Delegated with Up/Down

ARIN - American Registry

rpki1.dev.arin.net:8080/public/secure/org/rpki/updown/requestCertificate.xhtml?orgHandle=SPRN&conversationId=9

Google YouTube Berlin demo AOL more AOL Current Misc ARIN Webmail ARIN Voicemail User

ARIN
American Registry for Internet Numbers

SEARCH Whois
all requests subject to [terms of use](#) [advanced search](#)

NUMBER RESOURCES PARTICIPATE POLICIES FEES & INVOICES KNOWLEDGE ABOUT US

Welcome, Developer

MESSAGE CENTER (1)

WEB ACCOUNT

POC RECORDS

ORGANIZATION DATA

MANAGE & REQUEST RESOURCES

MEMBERSHIP APPLICATION

TRACK TICKETS

DOWNLOADS & SERVICES

ASK ARIN

[log out](#)

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: SPRN.identity.xml

Submit

Contact Us Terms of Service Media Site Map Search ARIN Privacy Statement Accessibility Network Abuse

© Copyright 1997 - 2013, American Registry for Internet Numbers

Delegated with Up/Down

The screenshot shows a web browser window with the URL `rpki1.dev.arin.net:8080/public/communication/ticket/view.xhtml?ticketNo=20130830-X1`. The browser's address bar and tabs are visible at the top. The page content is divided into several sections. On the left, there is a vertical orange bar. The main content area on the right contains a table of resource classes and a log of activities.

Resource Class	Resource Class	Resource Class
APNIC	RIPE	

Resource Class: APNIC
Certifiable Net(s): NET-209-235-96-0-2

Resource Class: RIPE
Certifiable Net(s): NET-216-205-64-0-1

Resource Class: RIPE
Certifiable Net(s): NET-216-205-144-0-1

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 CA
- Have a highly available repository
- Create a CPS

Updates within RPKI outside of ARIN

- The four other RIRs are in production with Hosted CA services
- ARIN and APNIC have delegated working for the public
- Major routing vendor support being tested
- Announcement of public domain routing code support

ARIN Status

- Hosted CA deployed 15 Sept 2012
- Web Delegated CA deployed 16 Feb 2013 (deprecated from lack of use)
- Delegated using “Up/Down” protocol deployed 7 Sept 2013
- RESTful interface deployed 1 Feb 2014

RPKI Usage

	Oct 2012	Apr 2013	Oct 2013	Apr 2014	Oct 2014	Apr 2015	Oct 2015
RPAs Signed	27	72	130	162	208	289	358
Certified Orgs		47	68	108	153	187	220
ROAs	19	60	106	162	239	308	338
Covered Resources	30	82	147	258	332	430	482
Up/Down Delegated			0	0	0	1	2

Why is this important?

- Provides more credibility to identify resource holders
- Leads to better routing security

Q&A

