



# ARIN NANOG

---

ON THE ROAD

**San Diego, California**  
25 February 2014

# Securing Routing: RPKI Overview

**Mark Kusters**  
Chief Technology Officer

## Why are DNSSEC and RPKI important?

- Two of the most critical resources
  - DNS
  - Routing
- Hard to tell when resource is compromised
- Focus of increased attention globally

# 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
- Authority to manage reverse zones follows SWIP
  - “Shared Authority” model

# 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.
```

## 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

# 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	HOSTNAMES OF NAMESERVERS
<u>252.149.192.in-addr.arpa.</u>	Nameserver 1: <input type="text" value="NS1.ARIN.NET"/>
	Nameserver 2: <input type="text" value="NS2.ARIN.NET"/>
	Nameserver 3: <input type="text" value="NS2.LACNIC.NET"/>
	Nameserver 4: <input type="text" value="SEC1.APNIC.NET"/>
	Nameserver 5: <input type="text" value="SEC1.AUTHDNS.RIPE.NET"/>
	Nameserver 6: <input type="text"/>
	Nameserver 13: <input type="text"/>

# 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 Management and DNSSEC in ARIN Online

- Available on ARIN's website

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



Using  
**ARIN  
ONLINE**

for Delegation Management  
and DNSSEC



**Click To Play**

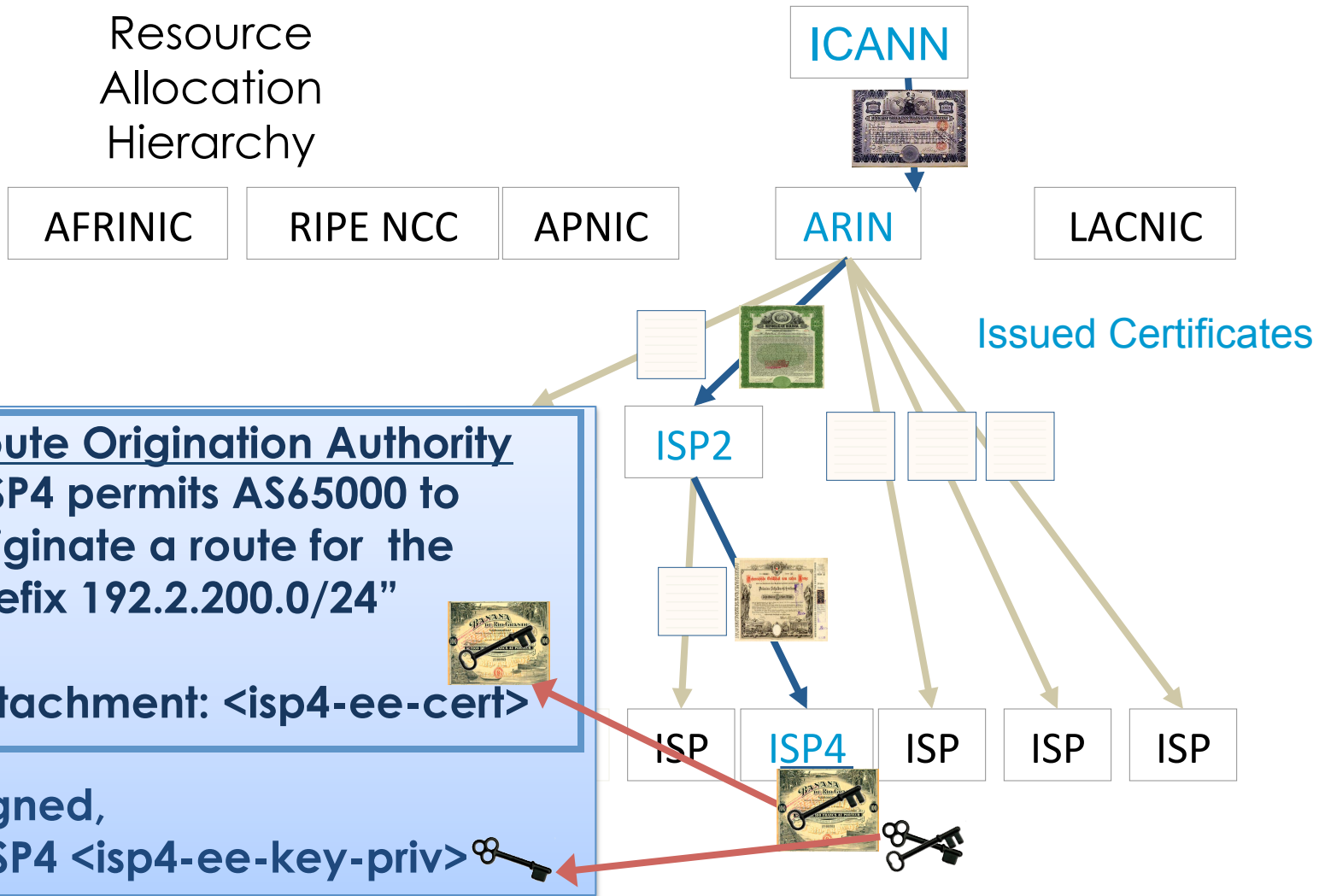
# What is RPKI?

- **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

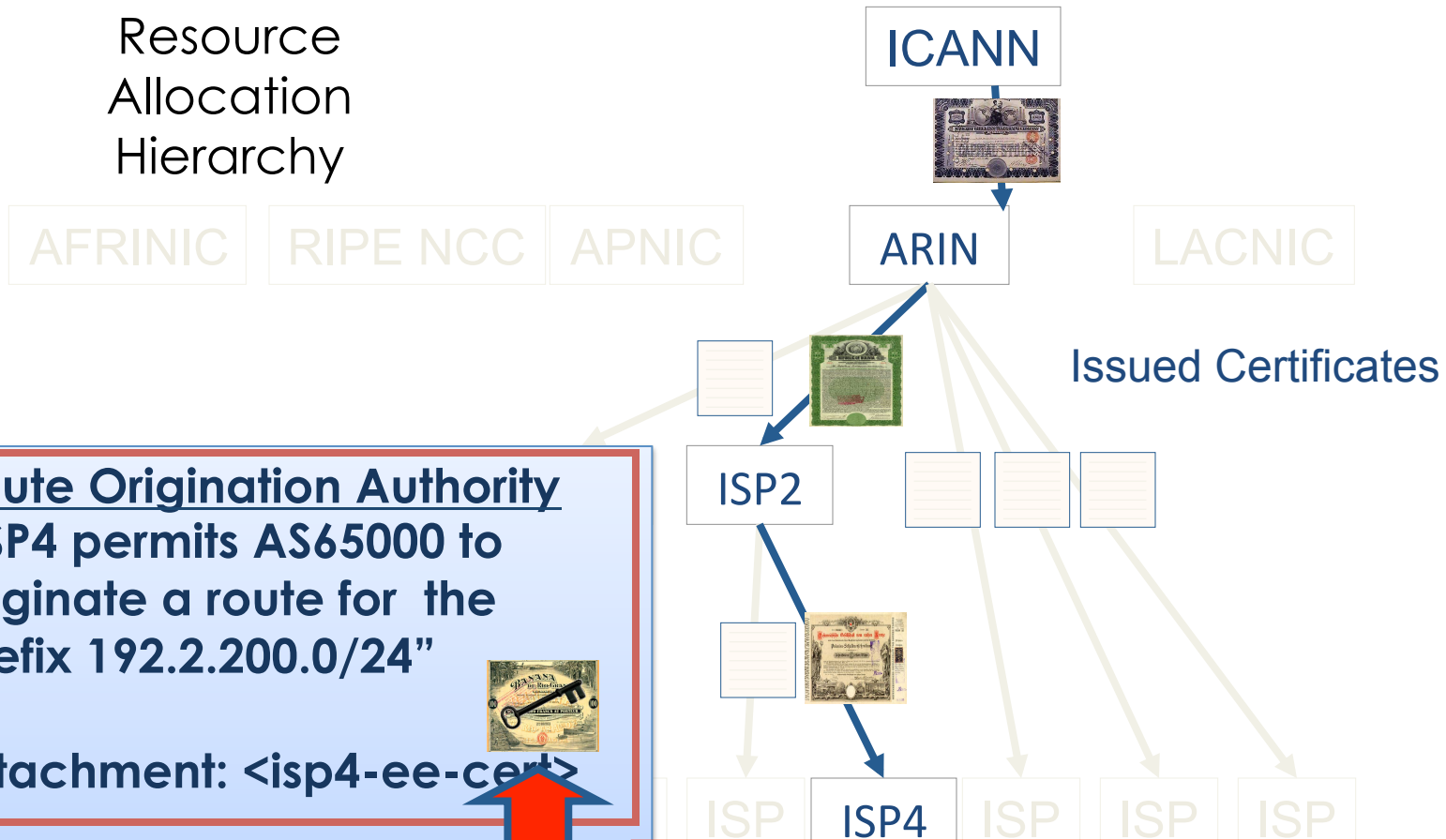
# What does RPKI accomplish?

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

Resource  
Allocation  
Hierarchy



Resource  
Allocation  
Hierarchy



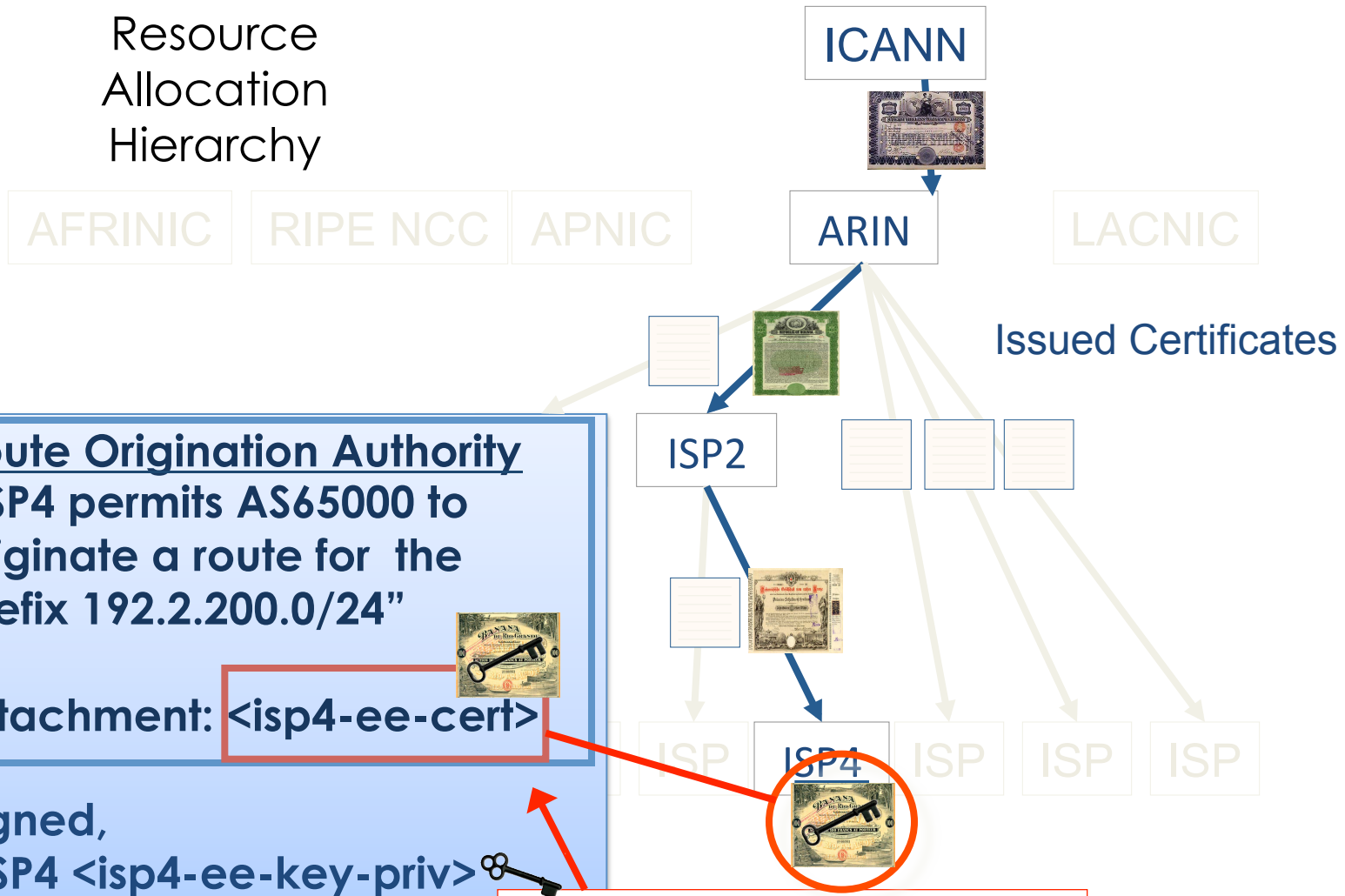
**Route Origination Authority**  
"ISP4 permits AS65000 to originate a route for the prefix 192.2.200.0/24"

Attachment: `<isp4-ee-cert>`

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

1. Did the matching private key sign this text?

Resource  
Allocation  
Hierarchy



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

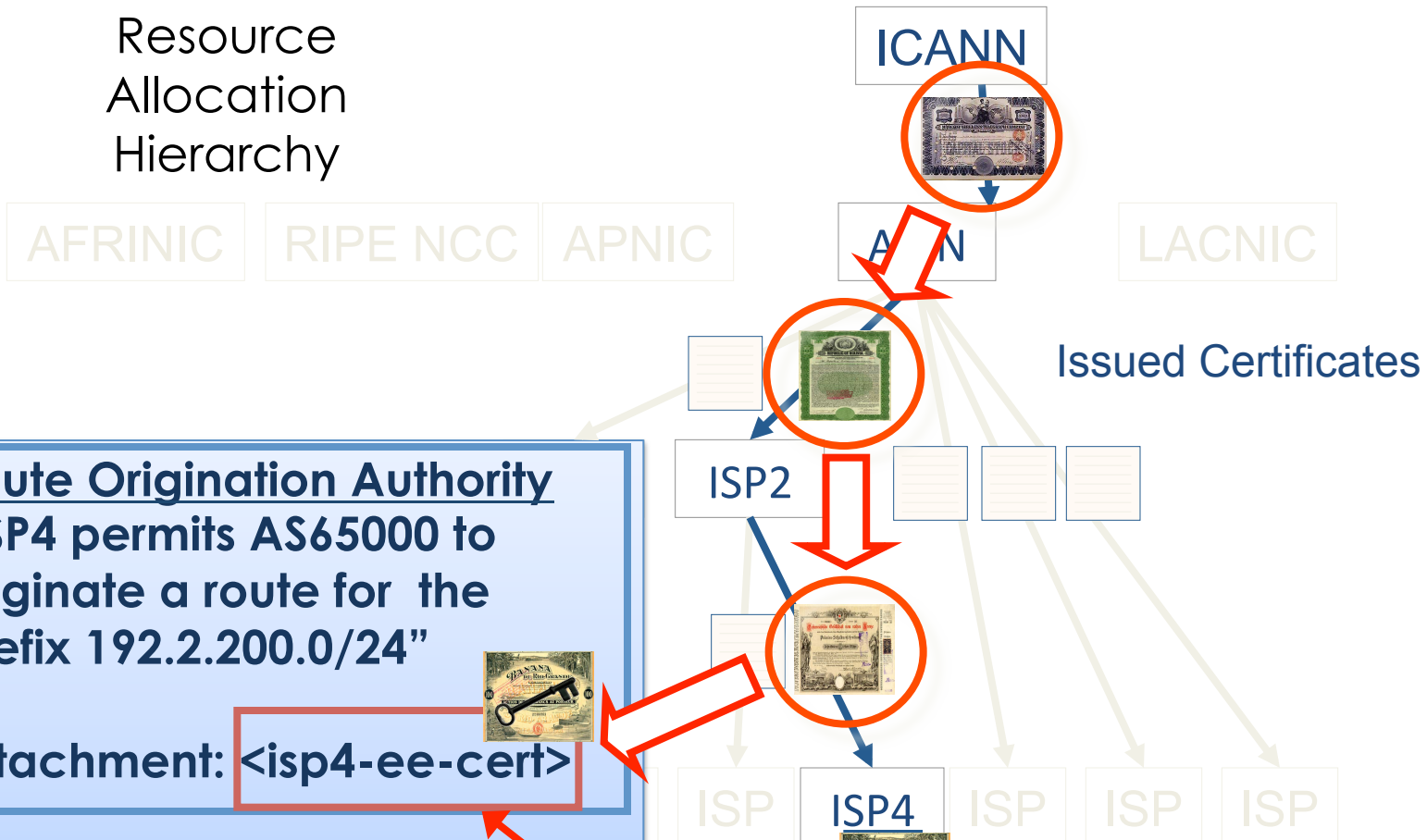
Attachment: `<isp4-ee-cert>`

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

2. Is this certificate valid?



Resource  
Allocation  
Hierarchy



**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 Flow

- 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
- Web Delegated
- 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



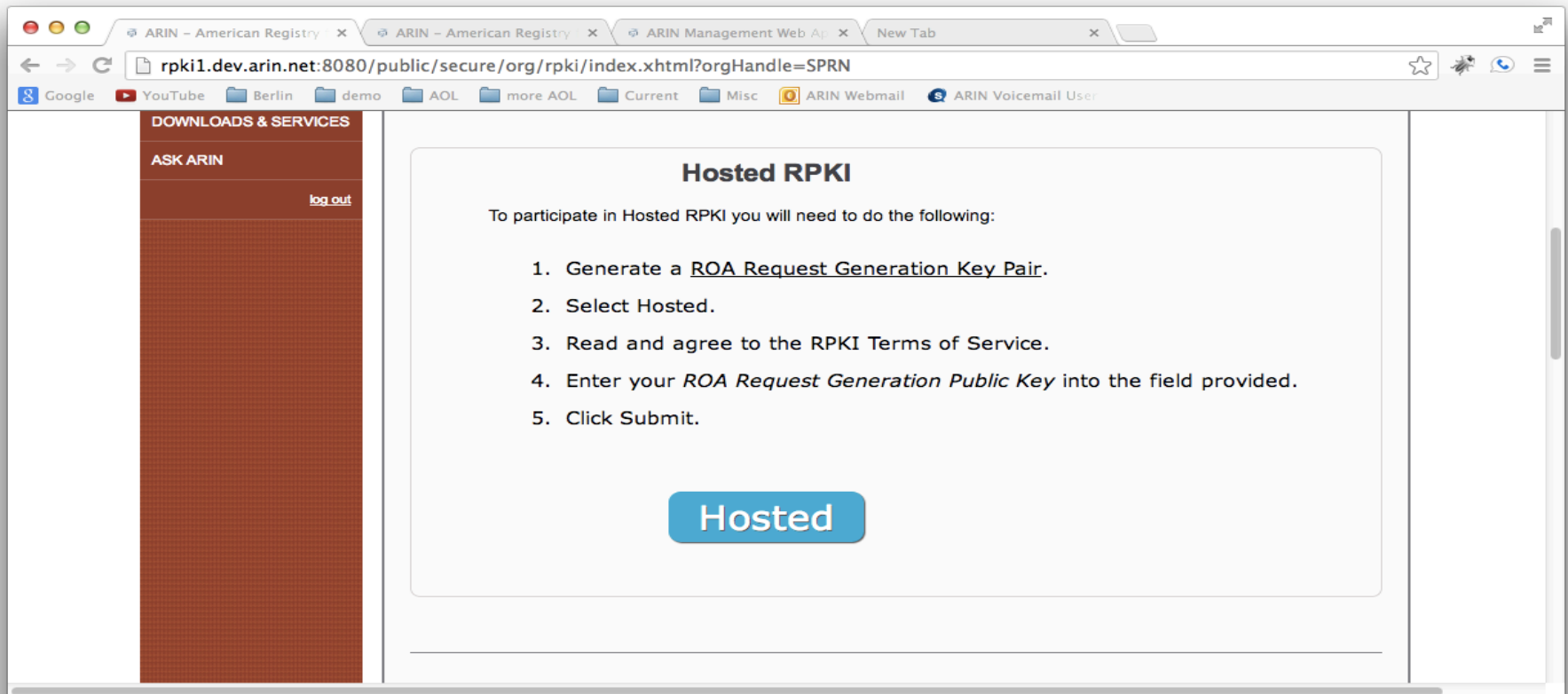
# Web Delegated RPKI

- Pros
  - Harder than Hosted, Easier than Delegated (Up/Down)
  - Manage your own RPKI system
  - Control your own private keys
- Cons
  - Need to setup your own RPKI environment
  - Fairly complex

# Delegated RPKI with Up/Down

- Pros
  - Same as web delegated
  - 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 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-----  
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvBhoSmbRQhbSpTIM2Pqn  
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 <sup>\*</sup>  add ?

Private Key:   Key Not Loaded

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**

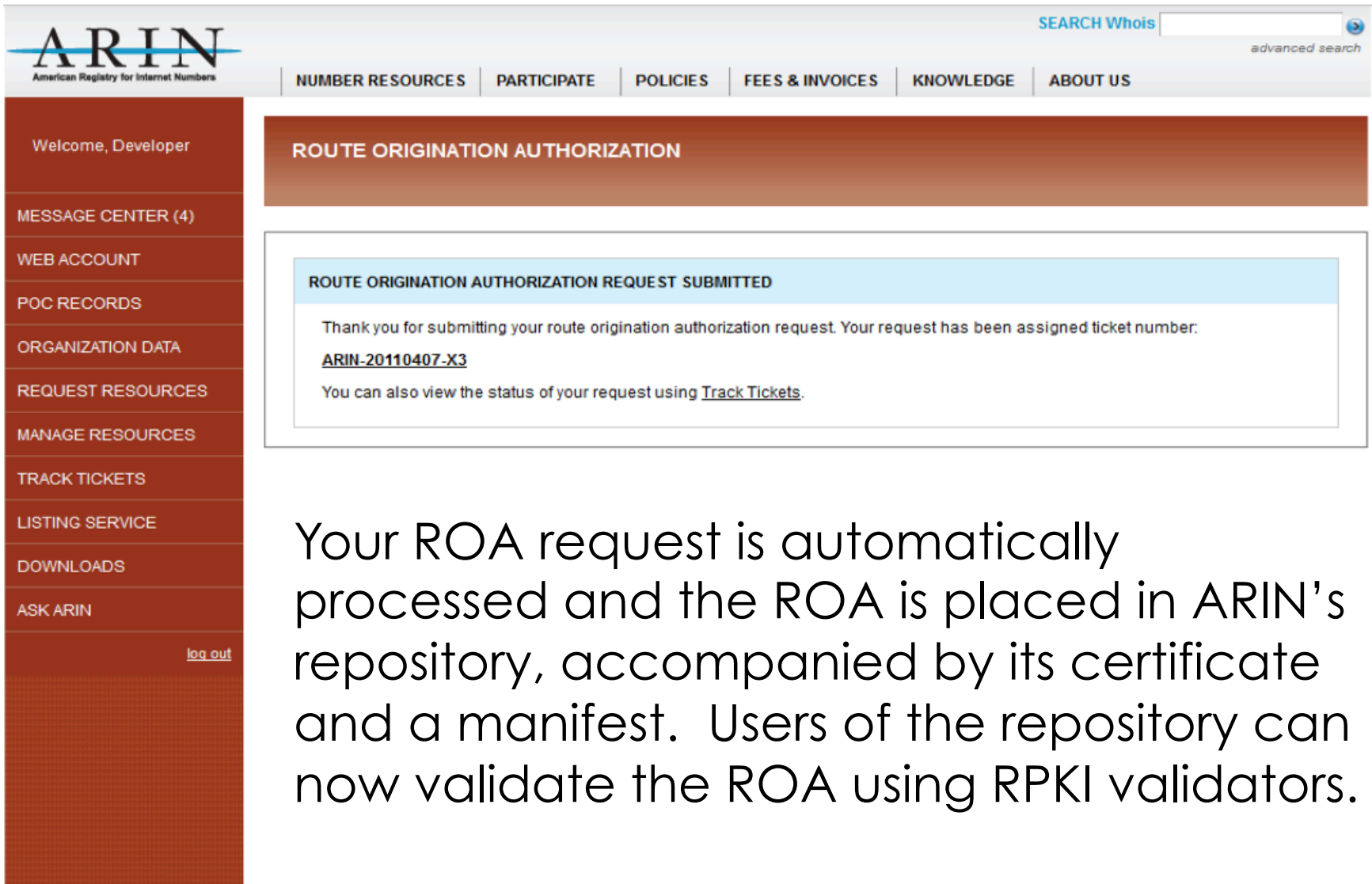
Validity Period: **03-20-2013 to 03-20-2023**

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

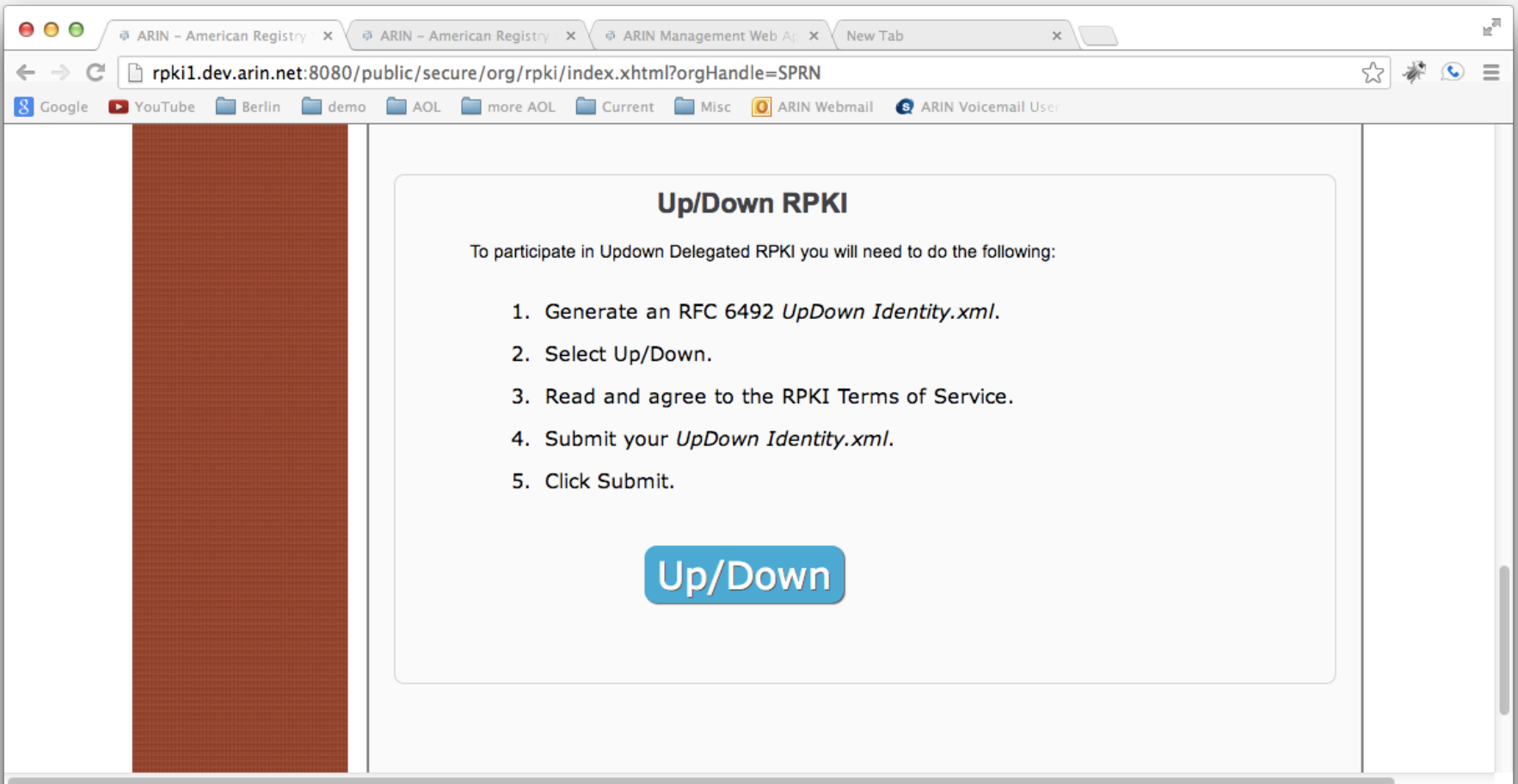
Submit Signed ROA Request



The screenshot shows the ARIN website interface. At the top left is the ARIN logo with the tagline "American Registry for Internet Numbers". To the right is a search bar labeled "SEARCH Whois" with a search button and a link to "advanced search". Below the logo is a horizontal navigation menu with items: "NUMBER RESOURCES", "PARTICIPATE", "POLICIES", "FEES & INVOICES", "KNOWLEDGE", and "ABOUT US". On the left side, there is a vertical sidebar menu with items: "Welcome, Developer", "MESSAGE CENTER (4)", "WEB ACCOUNT", "POC RECORDS", "ORGANIZATION DATA", "REQUEST RESOURCES", "MANAGE RESOURCES", "TRACK TICKETS", "LISTING SERVICE", "DOWNLOADS", and "ASK ARIN". At the bottom of the sidebar is a "log out" link. The main content area has a dark red header with the text "ROUTE ORIGINATION AUTHORIZATION". Below this is a light blue box containing the message: "ROUTE ORIGINATION AUTHORIZATION REQUEST SUBMITTED". The text inside the box reads: "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.

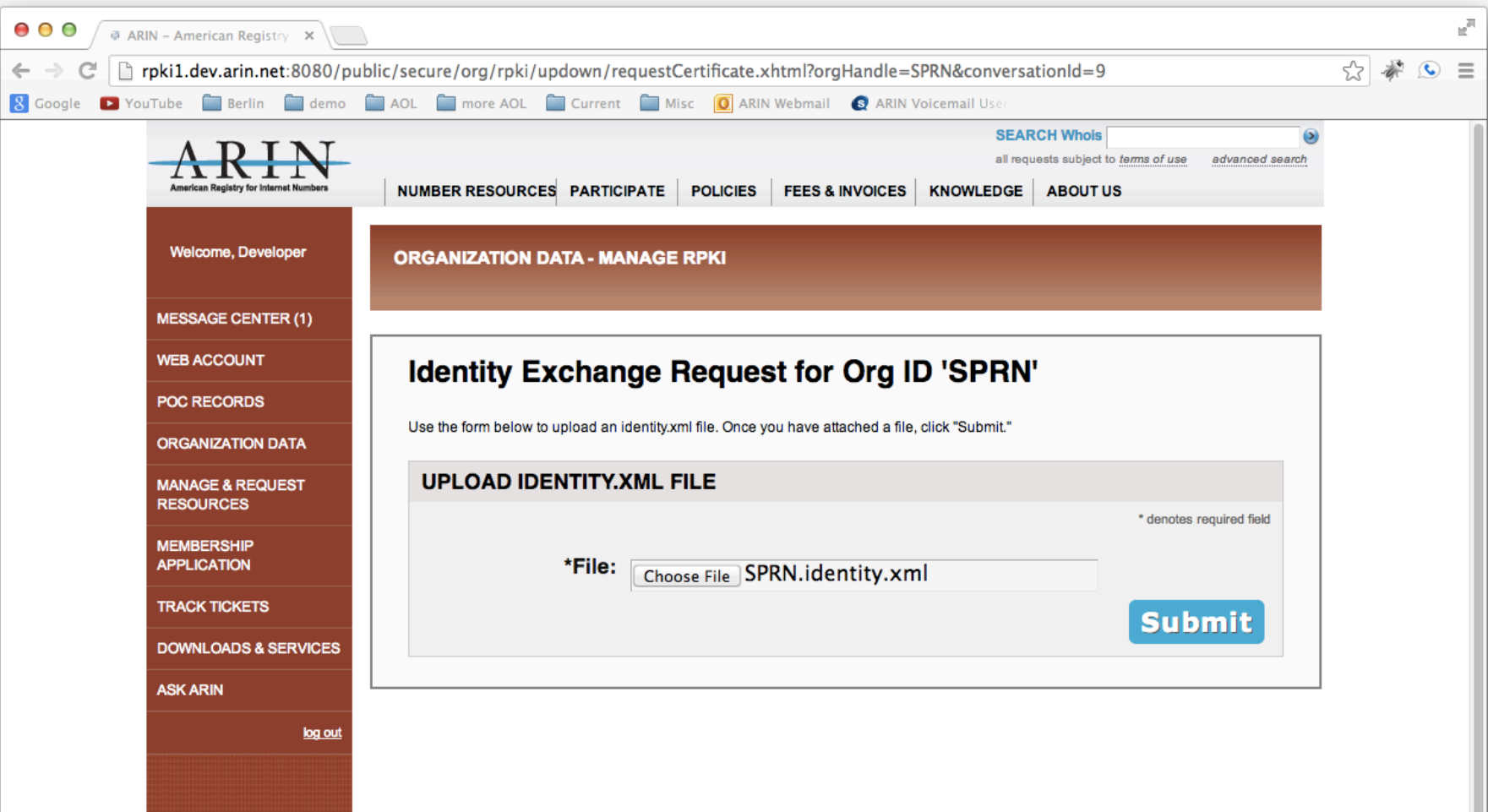
# Delegated with Up/Down



The screenshot shows a web browser window with the following details:

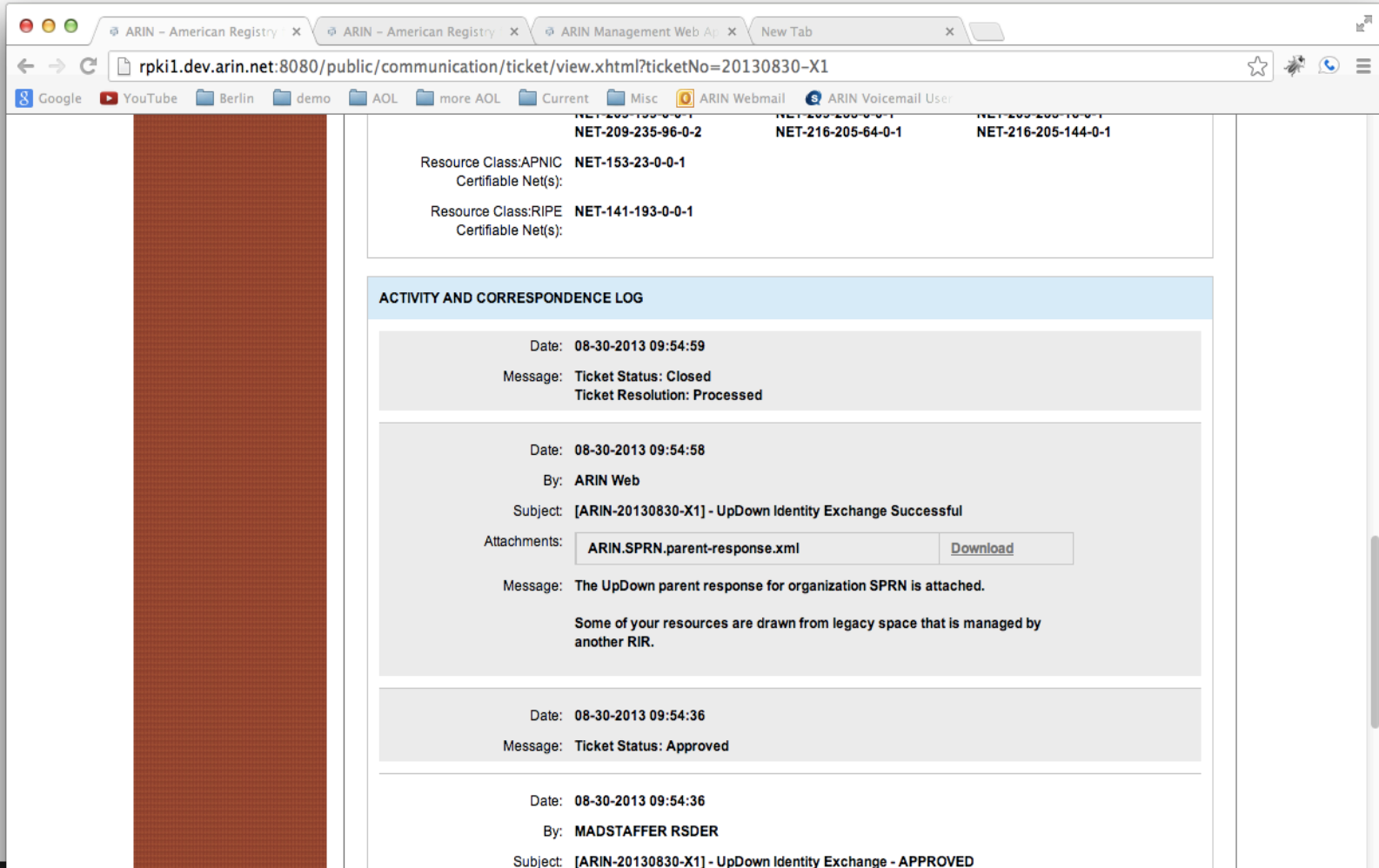
- Browser tabs: ARIN - American Registry, ARIN - American Registry, ARIN Management Web Ap, New Tab
- Address bar: `rpk1.dev.arin.net:8080/public/secure/org/rpki/index.xhtml?orgHandle=SPRN`
- Bookmarks: Google, YouTube, Berlin, demo, AOL, more AOL, Current, Misc, ARIN Webmail, ARIN Voicemail User
- Page Content:
  - 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.
  - [Up/Down](#) (button)

# Delegated with Up/Down



The screenshot shows a web browser window with the ARIN website. The browser's address bar displays the URL: `rpki1.dev.arin.net:8080/public/secure/org/rpki/updown/requestCertificate.xhtml?orgHandle=SPRN&conversationId=9`. The website header includes the ARIN logo and navigation links: NUMBER RESOURCES, PARTICIPATE, POLICIES, FEES & INVOICES, KNOWLEDGE, and ABOUT US. A search bar for 'SEARCH Whois' is also present. The left sidebar contains a navigation menu with items like 'Welcome, Developer', 'MESSAGE CENTER (1)', 'WEB ACCOUNT', 'POC RECORDS', 'ORGANIZATION DATA', 'MANAGE & REQUEST RESOURCES', 'MEMBERSHIP APPLICATION', 'TRACK TICKETS', 'DOWNLOADS & SERVICES', and 'ASK ARIN'. The main content area is titled 'ORGANIZATION DATA - MANAGE RPKI' and features a section for 'Identity Exchange Request for Org ID 'SPRN''. Below this title, there is a text prompt: 'Use the form below to upload an identity.xml file. Once you have attached a file, click "Submit."' The form itself is titled 'UPLOAD IDENTITY.XML FILE' and contains a file upload field with a 'Choose File' button and the filename 'SPRN.identity.xml'. A 'Submit' button is located to the right of the file field. A note '\* denotes required field' is visible in the top right corner of the form area.

# Delegated with Up/Down



The screenshot shows a web browser window with the following details:

- Browser tabs: ARIN - American Registry, ARIN Management Web A, New Tab
- Address bar: `rpki1.dev.arin.net:8080/public/communication/ticket/view.xhtml?ticketNo=20130830-X1`
- Navigation bar: Google, YouTube, Berlin, demo, AOL, more AOL, Current, Misc, ARIN Webmail, ARIN Voicemail User
- Table of resources:

Resource Class:APNIC	Resource Class:RIPE
NET-209-235-96-0-1	NET-153-23-0-0-1
NET-209-235-96-0-2	NET-141-193-0-0-1
NET-216-205-64-0-1	
NET-216-205-144-0-1	
- Section: **ACTIVITY AND CORRESPONDENCE LOG**
- Log entries:
  - 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
- Delegated using “Up/Down” protocol deployed 7 Sept 2013
- RESTful interface deployed 1 Feb 2014



# Why is this important?

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

# Q&A

