



# A Walking Tour of RPKI

Tim Christensen

24-26 Oct 2012

# Our Trail Map

- A little RPKI orienteering
- What path led us to here?
- Are we there yet?
- The path yet to come

# RPKI Orienteering

- ...navigating from point to point, in diverse and usually unfamiliar terrain, normally moving at speed

# RPKI Orienteering

- Resource Public Key Infrastructure
- Issues certificates for network resources to resource holders
  - **AS Numbers**
  - **IP Addresses**
- Allows network holders to associate the two via a Route Origin Authorization (ROA)
- Allows relying parties to validate authenticity and effectivity of signed objects

# RPKI Orienteering

- Can be used as “reliable trust model” for route origin announcements for routing decisions
- Could be used by routers to validate origin
- Needs minimal bootstrap info
  - **Trust Anchor**
  - **Mechanism for validation**
- Managed through ARIN Online or REST



# RPKI Orienteering

- The RPKI system creates a repository:
  - **RFC 3779 (RPKI) Certificates**
  - **ROAs**
  - **CRLs**
  - **Manifest records**

# Rest Stop: The Repository

```
./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 dSmerM6uJGLWMMQT12esy4xyUAA.crl
-rw-r--r--  1 143  143  1882 Jun 26  2009 dSmerM6uJGLWMMQT12esy4xyUAA.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

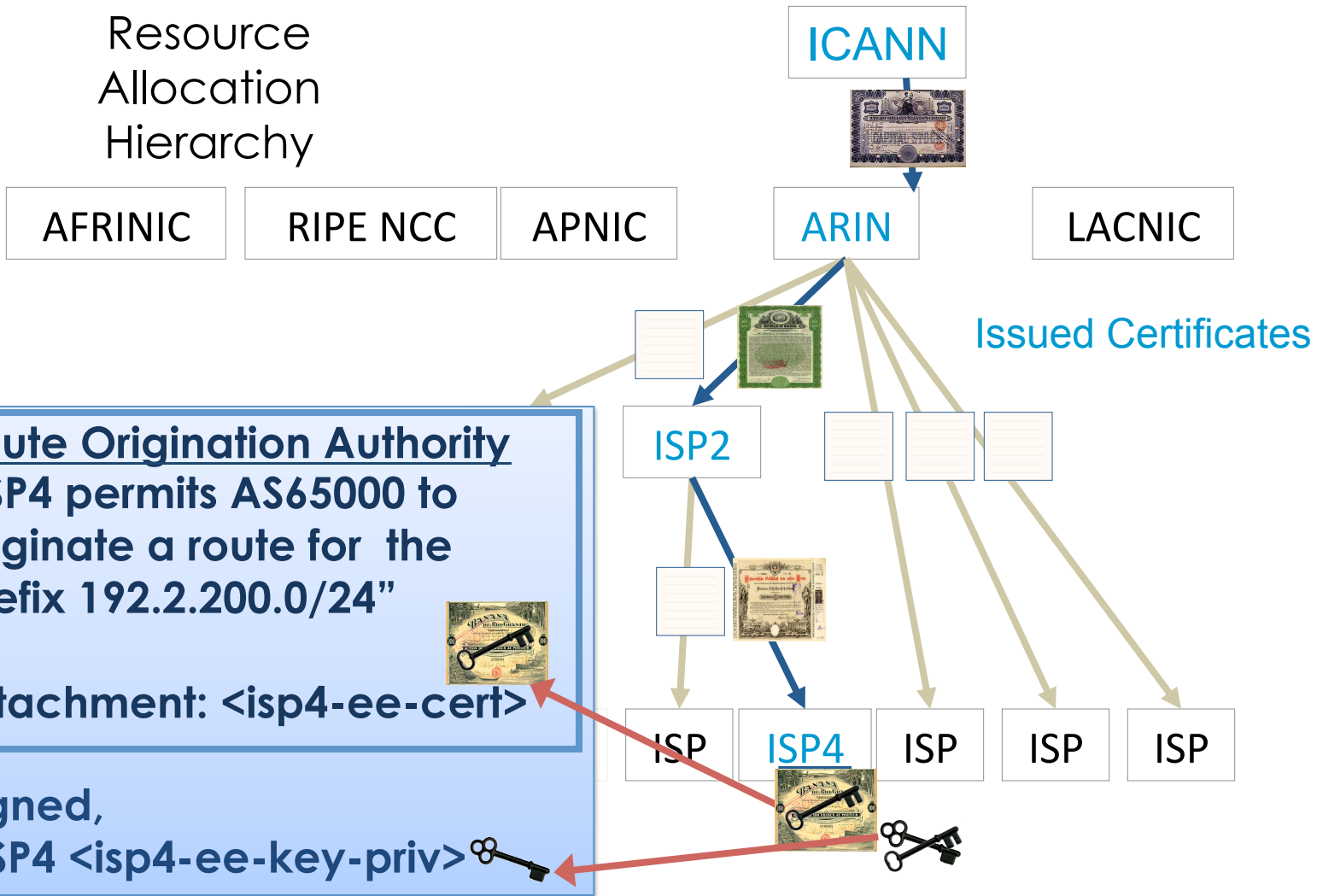
# Repository Use

- Shared via a distribution mechanism
- Validate objects (mainly ROAs) in the repository
- Can be used to communicate with routers for marking routes as valid, invalid, or unknown
- Entirely up to local policy how this content is used



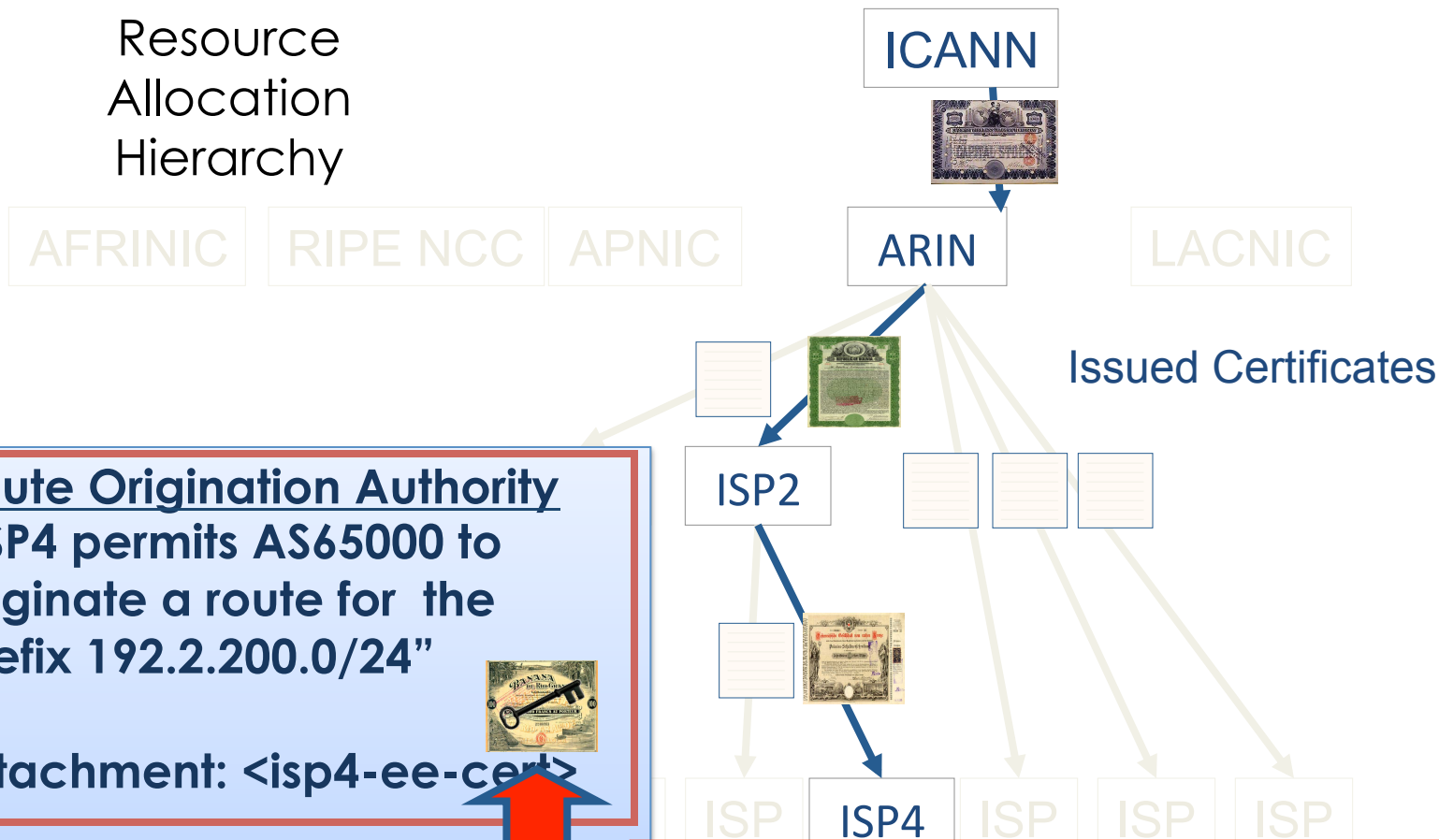
# ROA Validation

Resource  
Allocation  
Hierarchy



# ROA Validation

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?

# ROA Validation

Resource  
Allocation  
Hierarchy

AFRINIC

RIPE NCC

APNIC

ICANN



ARIN

LACNIC

Issued Certificates



ISP2



ISP

ISP4

ISP

ISP

ISP



**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?

ARINXXX DALLAS

# ROA Validation

Resource  
Allocation  
Hierarchy



ICANN



AN



ISP2



ISP

ISP4

ISP

ISP

ISP

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>**

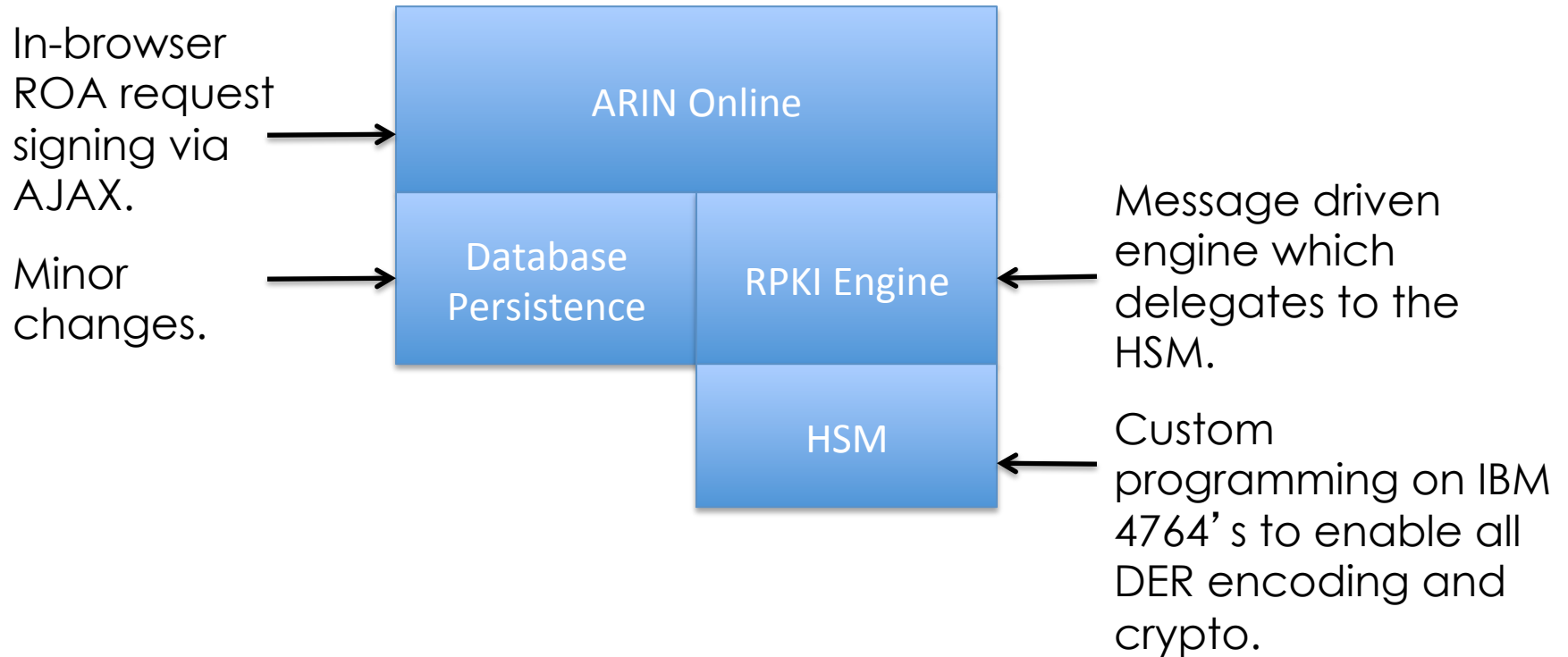
3. Is there a valid certificate path from a Trust Anchor to this certificate?

# What Path Led Us to Where We Are?

- Other four RIRs have had RPKI services for various amounts of time
- Specific concerns led ARIN down a customized path
  - Non-repudiation of ROA generation when ARIN performs this on behalf of a registrant
  - Protection from rogue insider



# The Road We've Trod



HSM coding is in C as extensions to IBM CCA.  
Libtasn1 used for DER encoding.

# Are We There Yet?

- RPKI services now offered thru ARIN Online and REST for a “hosted” model
- Repository publication is periodic
- Anyone can be a relying party
- A number of validators can be used to check validity of ROAs

# Pictures from the Road Trip

- Initiating Participation in RPKI
- Requesting a ROA once you receive your Certificate
- Requesting the TAL as a Relying Party
- Validating Content

# Take the First Step

## Information

Resource Public Key Infrastructure (RPKI) is a robust security framework for verifying the association between resource holders and their Internet resources using resource certificates.

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

1. Click "create resource certificate."
2. Accept the Terms of Service.
3. Submit your *ROA Request Generation* Public Key.
4. Submit a ROA Request signed with your *ROA Request Generation* Private Key.

[Learn more about RPKI.](#)

[Learn more about creating a ROA Request Generation Key Pair.](#)

## Manage RPKI



create resource  
certificate

# Step 1: Participating in RPKI

- Submit a ROA Request Generation Key Pair

– See

<https://www.arin.net/resources/rpki/faq.html#keypairgeneration>

– Looks like:

```
-----BEGIN PUBLIC KEY-----  
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzH/1ws2aiqyxR0tqpkAC  
tLGhQMrkYfcxYl7BzxFaseitdsNhxqNZjAt+IB/yQ9XEKaHL87cqmZlrtEGju0Dk  
QKym0onn3JXtS7S1OTRQbjWPN0k9/1HnP/R5xnQvGfAMOPm9S5If6DPr63109inX 5JXv4yNx/x8GZAT+RrhrW  
/I+PzmXVeSwc89LbADblpQR5x9x6173ncHUV+6UJr2M  
niBl7OcFW61jbGhTQSRb9xoUli7IyAciziESE6cG2gqw0fW/ZOo7pUToPaDAPxHJ  
vLq0uqtlpG5z3MpAoVibtduF9BF2dKHFF6TMwUKJaQ5EQZ+/iODk6CuWz6Q5iZN  
GwIDAQAB  
-----END PUBLIC KEY-----
```



# Step 1: Participating in RPKI

- You will get an RPKI Certificate

Welcome, Tim

MESSAGE CENTER

WEB ACCOUNT

POC RECORDS

ORGANIZATION DATA

MANAGE & REQUEST RESOURCES

BILLING INFO

MEMBERSHIP APPLICATION

TRACK TICKETS

DOWNLOADS & SERVICES

## ORGANIZATION DATA - MANAGE RPKI

### Information

Resource Public Key Infrastructure (RPKI) is a robust security framework for verifying the association between resource holders and their Internet resources using resource certificates.

[Learn more about RPKI.](#)

[Learn more about creating a ROA Request Generation Key Pair.](#)

### RESOURCE CERTIFICATE FOR ORG ID 'ARINOPS'

Issuer: **CN=2a246947-2d62-4a6c-ba05-87187f0099b2**  
Subject: **CN=ad6556d7-60a4-4318-9d11-464fb8396d3e**  
Serial: **4439943689693081523527336919011583791657145776**  
Validity: **09-15-2012 to 09-15-2022**

### Manage RPKI



create roa

# Step 2: Requesting a ROA

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](#)

## CREATE A ROUTE ORIENTATION AUTHORIZATION

There are two ways to submit a Route Origination Authorization (ROA) request

**Browser Signed ROA Request:** Allows you enter in each required field separately and digitally sign the request with your RSA private key within the browser.

**Signed ROA Request:** Allows you to submit a digitally signed ROA request. This method requires you to construct a precisely formatted text block containing your ROA request information, and then to sign it with and RSA private key which you create. More details on the formatting requirements are provided in a link in the signed ROA tab.

**Submit Browser Signed ROA** | **Submit Signed ROA**

\*Name:

\*Origin AS:  \* denotes required field

\*Validity Start Date:   
Enter the date in mm/dd/yyyy format.

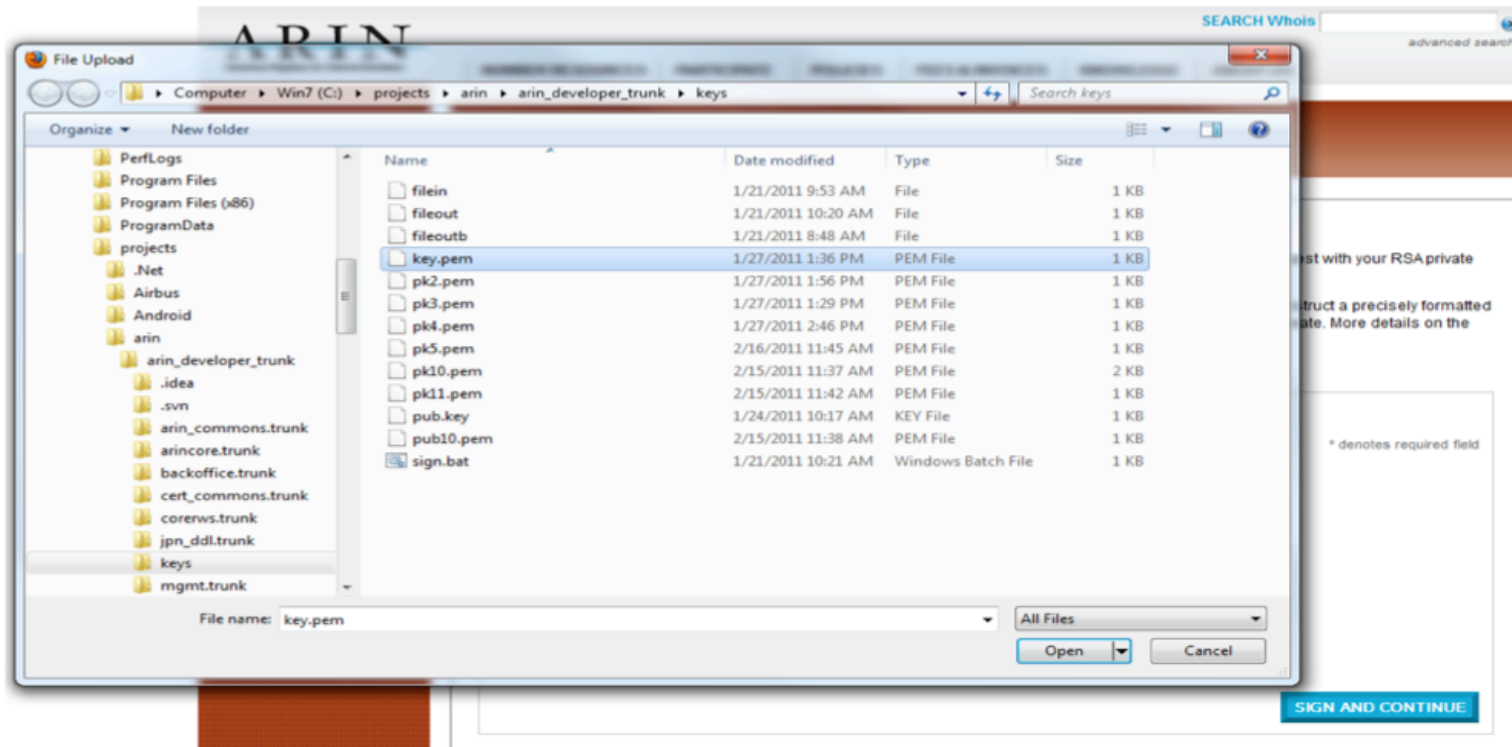
\*Validity End Date:   
Enter the date in mm/dd/yyyy format.

Prefix:  /  Max Length  [Add](#)


Select Signing Private Key:

This key will not be uploaded to ARIN.

# Step 2: Requesting a ROA



# Step 2: Requesting a ROA



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](#)

## CREATE A ROUTE ORIENTATION AUTHORIZATION

There are two ways to submit a Route Origination Authorization (ROA) request.

**Browser Signed ROA Request:** Allows you enter in each required field separately and digitally sign the request with your RSA private key within the browser.

**Signed ROA Request:** Allows you to submit a digitally signed ROA request. This method requires you to construct a precisely formatted text block containing your ROA request information, and then to sign it with and RSA private key which you create. More details on the formatting requirements are provided in a link in the signed ROA tab.

**Submit Browser Signed ROA** | **Submit Signed ROA**

\*Name:

\*Origin AS:  \* denotes required field

\*Validity Start Date:   
Enter the date in mm/dd/yyyy format.

\*Validity End Date:   
Enter the date in mm/dd/yyyy format.

Prefix:  /  Max Length  [Add](#)

Select Signing Private Key: [Key Loaded](#)  
[Click to Remove](#)

This key will not be uploaded to ARIN.

[SIGN AND CONTINUE](#)



# Step 2: Requesting a ROA

**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](#)

## CREATE A ROUTE ORIGINATION AUTHORIZATION

### SUBMIT SIGNED ROUTE ORIGINATION AUTHORIZATION

Verify the information below matches the request you wish to submit, then click the button below. *Note: Your digital signature will not be validated until you click the button below.*

Name: **Test ROA**

Origin AS: **123**

Validity Period: **04-07-2011 - 04-07-2015**

Resources: **174.128.0.0/23**

Signature: **vGNHCrOlqDUGfcJzRWwhJVITPKeyxhWtt79pyqa3UJI SuhFbuh ZVQdlhJ1uRZszmmCM33EvOI6QoO/HMUw+WPw==**

[SUBMIT SIGNED ROA REQUEST](#)



# Step 2: Requesting a ROA

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 navigation menu with links for "NUMBER RESOURCES", "PARTICIPATE", "POLICIES", "FEES & INVOICES", "KNOWLEDGE", and "ABOUT US". On the left side, there is a vertical sidebar menu with the following items: "Welcome, Developer", "MESSAGE CENTER (4)", "WEB ACCOUNT", "POC RECORDS", "ORGANIZATION DATA", "REQUEST RESOURCES", "MANAGE RESOURCES", "TRACK TICKETS", "LISTING SERVICE", "DOWNLOADS", "ASK ARIN", and a "log out" link at the bottom. The main content area features a dark red header with the text "ROUTE ORIGINATION AUTHORIZATION". Below this is a light blue confirmation box with the following text: "ROUTE ORIGINATION AUTHORIZATION REQUEST SUBMITTED", "Thank you for submitting your route origination authorization request. Your request has been assigned ticket number: **ARIN-20110407-X3**", and "You can also view the status of your request using [Track Tickets](#)."

# Step 3: Becoming a Relying Party

## RPKI - TRUST ANCHOR LOCATOR

### ARIN Relying Party Agreement

The Trust Anchor Locator (TAL) is used to retrieve and verify ARIN's Resource Public Key Infrastructure (RPKI) Repository. Any user may request to receive the TAL. You do not need to be logged in to ARIN Online in order to submit the request. However, you must agree to the ARIN Relying Party Agreement (RPA).

#### AGREEMENT

- I agree to the terms of the ARIN Relying Party Agreement  
You must accept the Relying Party Agreement in order to proceed.

CONTINUE

#### RELYING PARTY AGREEMENT

**AMERICAN REGISTRY FOR INTERNET NUMBERS, LTD.  
RESOURCE CERTIFICATION RELYING PARTY AGREEMENT**

YOU MUST READ AND ACCEPT THIS RESOURCE CERTIFICATION RELYING PARTY AGREEMENT (THIS "AGREEMENT") BEFORE ACCESSING OR USING ANY ONLINE RESOURCE CERTIFICATION PKI ("ORCP") SERVICES (AS DEFINED BELOW).

# Step 3: Becoming a Relying Party

## RPKI - TRUST ANCHOR LOCATOR

### ARIN RPKI Trust Anchor Locator

ARIN will email the Trust Anchor Locator (TAL) to the email address you provide below.

#### INFO

\*Email Address:

#### SECURITY

\*What is 0 + 9:

The mathematical equation enables us to distinguish if you are a human or a malicious bot.

[CONTINUE](#)


# Step 3: Becoming a Relying Party

## RPKI - TRUST ANCHOR LOCATOR


### ARIN RPKI TRUST ANCHOR LOCATOR REQUEST SUBMITTED

Thank you for submitting your request to receive the ARIN RPKI Trust Anchor Locator (TAL). ARIN will send an email message containing the TAL to the email address you provided in your request.

# Step 4: Validate Content

RPKI Validator Home Trust Anchors **ROAs** Ignore Filters Whitelist BGP Preview Export Router Sessions 

## Validated ROAs

Validated ROAs from arin. 

Show  entries

Search:

ASN	Prefix	Maximum Length	Trust Anchor
237	35.0.0.0/9	9	arin
237	2001:48a8::/32	32	arin
237	207.72.0.0/14	14	arin
237	192.122.181.0/24	24	arin
237	192.122.182.0/23	23	arin
237	204.38.0.0/15	15	arin
237	192.122.184.0/21	21	arin
237	198.108.0.0/14	14	arin
10745	199.43.0.0/24	24	arin
10745	192.136.136.0/24	24	arin

First Previous **1** 2 3 4 Next Last

Showing 1 to 10 of 31 entries



# Where Do We Go From Here?

- Validated content can be used to make decisions about routing
- There is a variety of work in this area
- Learn more about transferring RPKI data to Routers – read the RPKI-to-Router (RTR) Internet Draft at <http://tools.ietf.org/html/ietf-sidr-rpki-rtr-26>
- Local decisions always apply

# The Path Yet To Come

- Actively developing the “Delegated” model, if you want to run your very own Certificate Authority
- Requires a protocol for you to gain authority via RFC3779 Certificates that ARIN issues to you
- Provides a way for you to do your own thing with RPKI

**Thank You**