Changes at ARIN—Not your Grandpa's RIR anymore (RPKI, DNSSEC, etc.)

Andy Newton
Chief Engineer

Agenda

- DNSSEC – a brief update
- RPKI – the major focus
  - What is it
  - What it will look like within ARIN Online

Why are DNSSEC and RPKI Important?

- Two critical resources
  - DNS
  - Routing
- Hard to tell when resource is compromised
- Focus of Government funding - DHS

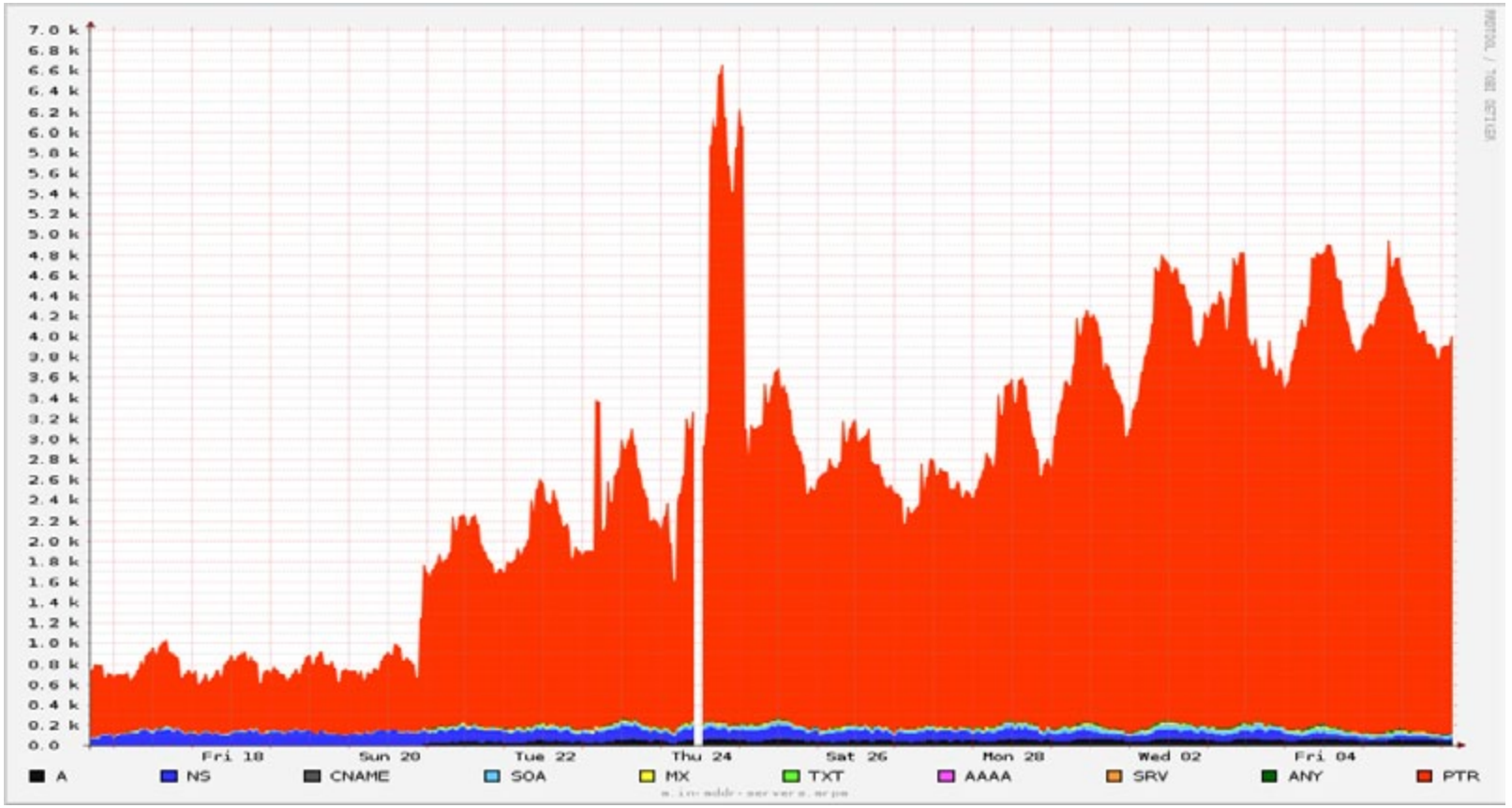
What is DNSSEC?

- DNS responses are not secure
  - Easy to Spoof
  - Examples of malicious attacks
- DNSSEC attaches signatures
  - Validates responses
  - Can not Spoof

Changes Required to make DNSSEC work

- Transfer of in-addr.arpa to ICANN
- Moving Nameservers for in-addr.arpa from the roots to RIR-managed systems
- Signing in-addr.arpa, ip6.arpa and delegations that ARIN manages
- Provisioning of DS Records
  - ARIN Online
  - RESTful Interface (just deployed on July 23)

Traffic from a.in-addr-servers.arpa



American Registry for Internet Numbers

Demo

- Movie from https://www.arin.net/knowledge/dnssec/

RPKI Pilot

- Available since June 2009
  - http://rpki-pilot.arin.net
  - ARIN-branded version of RIPE NCC software
- 46 organizations participating
- #2 (behind RIPE) on prefixes/roas

What is RPKI?

- Attaches certificates to network resources
  - AS Numbers
  - IP Addresses
- Allows ISPs to associate the two
  - Route Origin Authorizations (ROAs)
  - Follow the allocation chain to the top

What is RPKI?

- Allows routers to validate Origins
- Start of validated routing
- Need minimal bootstrap info
  - Trust Anchors
  - Lots of focus on Trust Anchors

What does RPKI Create?

- It creates a repository
  - RFC 3779 Certs
  - ROAs
  - CRLS
  - Manifest records
  - Ghostbusters support

Repository View

./ba/03a5be-ddf6-4340-a1f9-1ad3f2c39ee6/1:

total 40

-rw-r--r-- 1 markk markk 1543 Jun 26 2009 lCcaIRKhGHJ-TgUZv8GRKqkidR4.roa

-rw-r--r-- 1 markk markk 1403 Jun 26 2009 cKxLCU94umS-qD4DOOkAK0M2US0.cer

-rw-r--r-- 1 markk markk 485 Jun 26 2009 dSmerM6uJGLWMMQTl2esy4xyUAA.crl

-rw-r--r-- 1 markk markk 1882 Jun 26 2009 dSmerM6uJGLWMMQTl2esy4xyUAA.mnf

-rw-r--r-- 1 markk markk 1542 Jun 26 2009 nB0gDFtWffKk4VWgln-12pdFtE8.roa

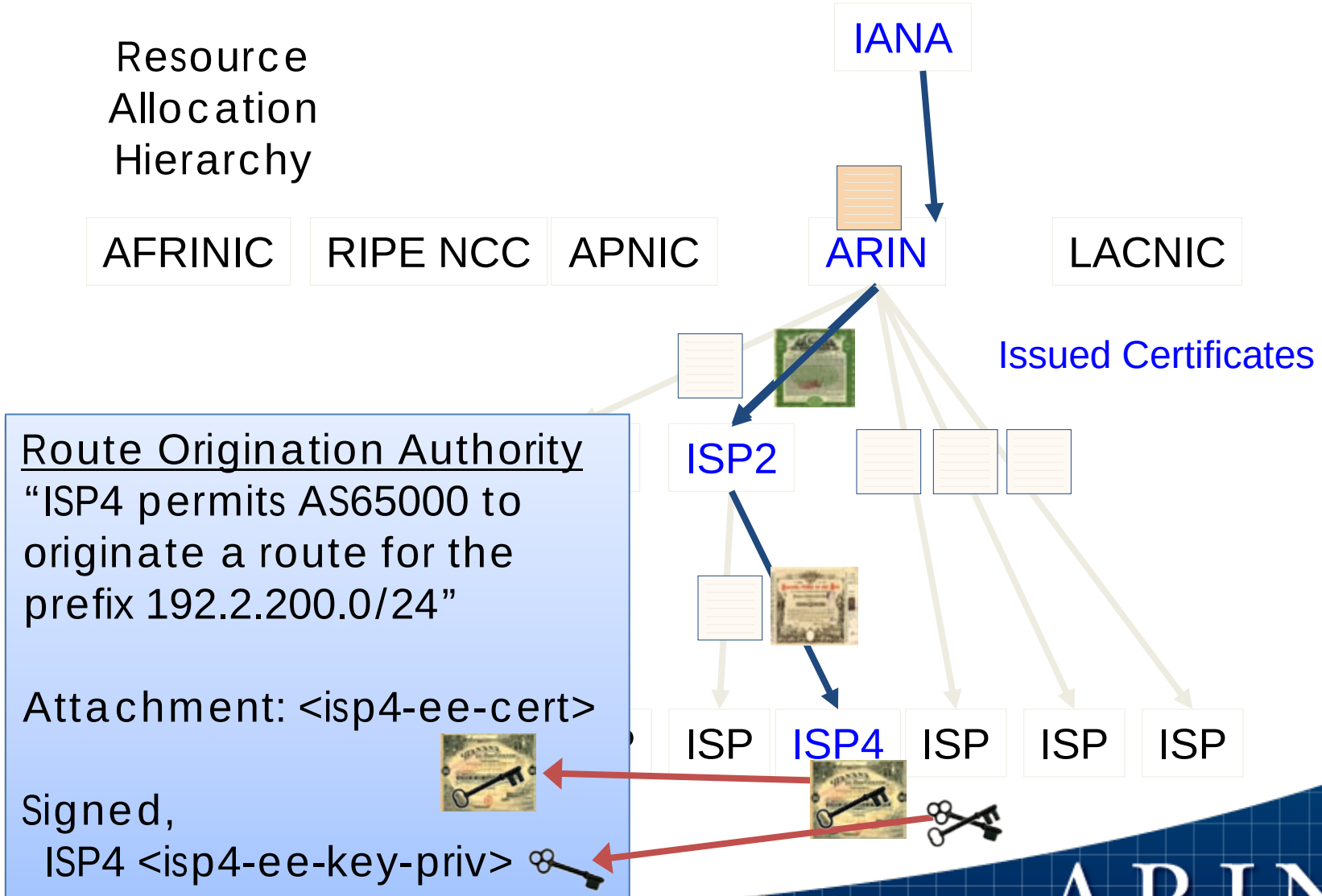
Repository Use

- Pull down these files using “rcynic”
- 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

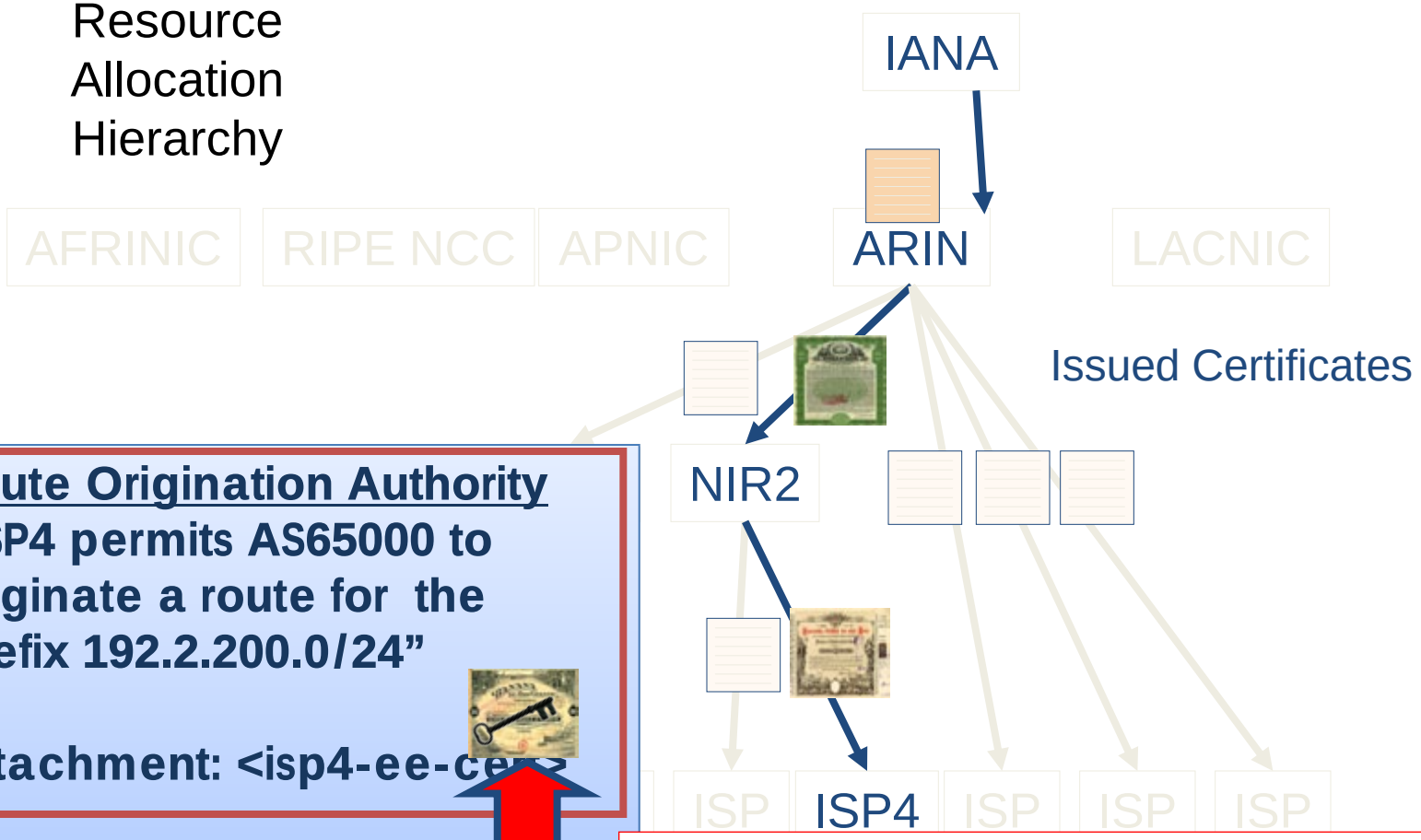
- RPKI web interface -> repository
- Repository aggregator -> validator
- Validated entries -> route checking
- Route checking results -> local routing decisions (based on local policy)

Resource Cert Validation



Resource Cert Validation

Resource
Allocation
Hierarchy



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

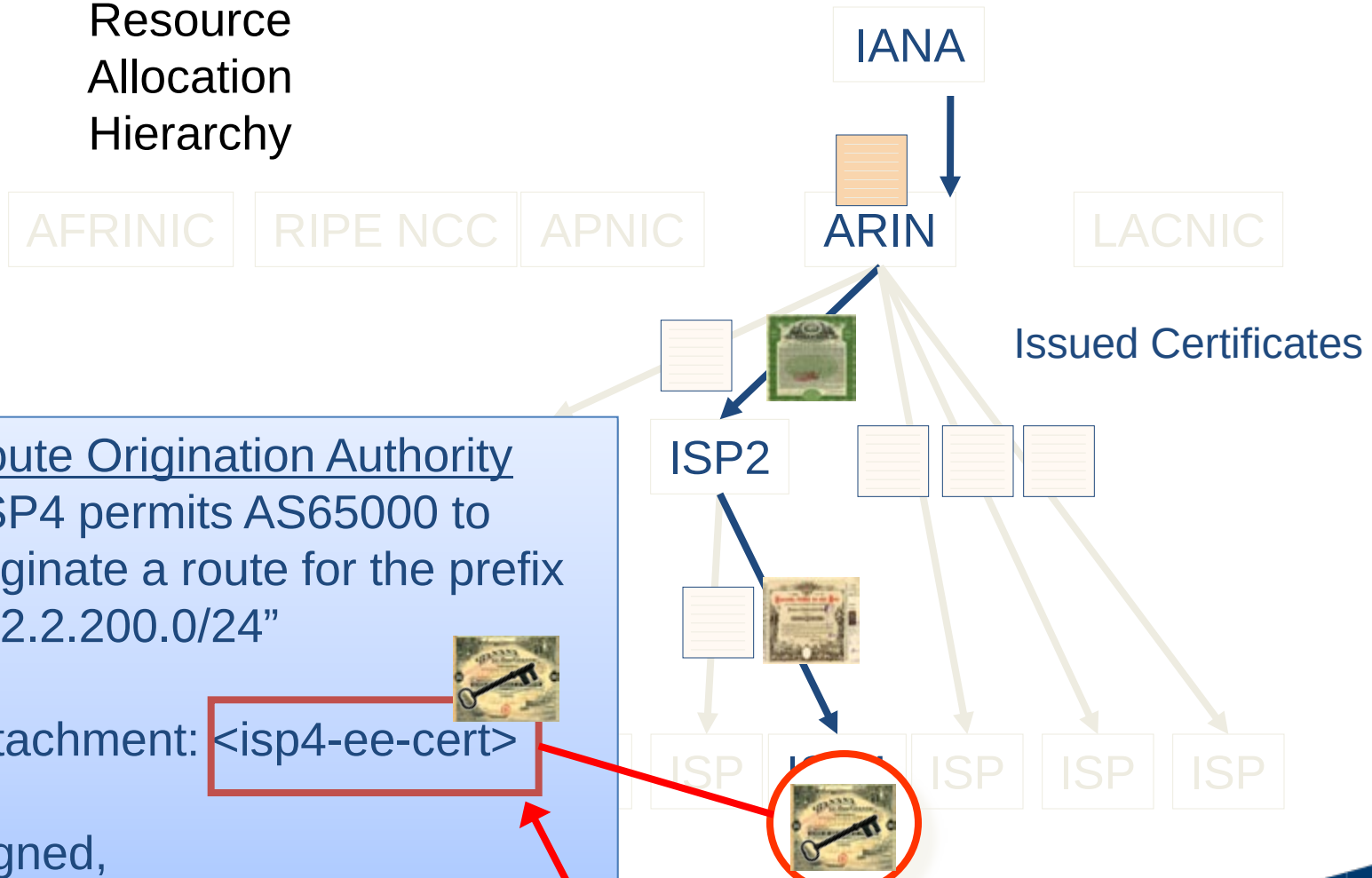
Attachment: <isp4-ee-cert>

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

1. Did the matching private key sign this text?

Resource Cert Validation

Resource
Allocation
Hierarchy



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

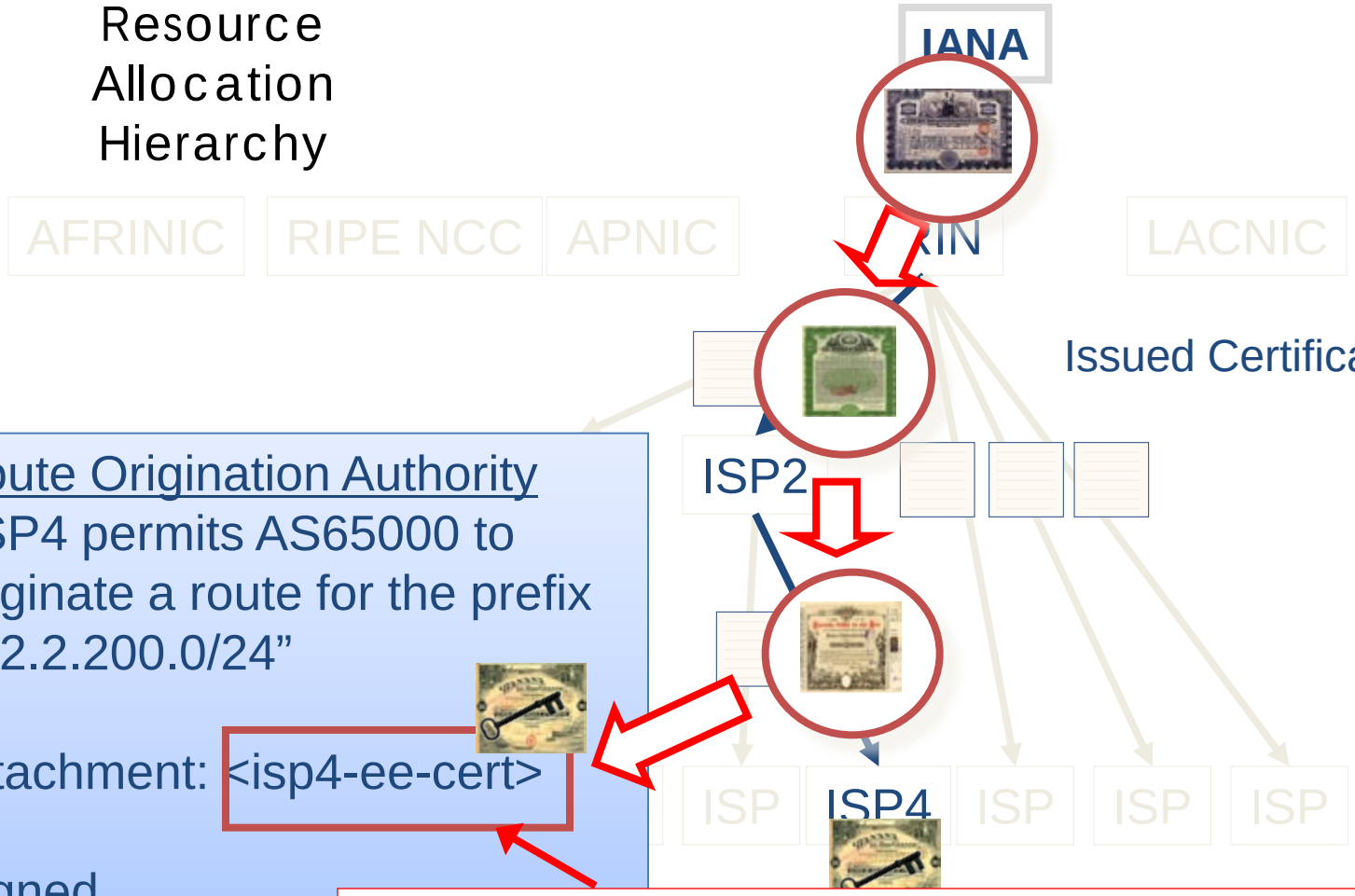
Attachment: <isp4-ee-cert>

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

2. Is this certificate valid?

Resource Cert 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>

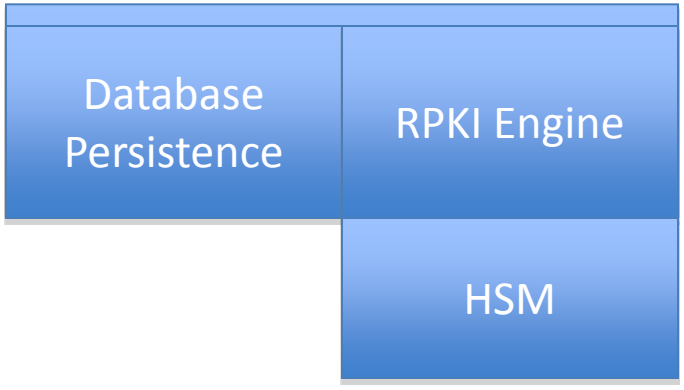
Signed,
ISP4 <isp4-ee-ke

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

Why is RPKI taking awhile?

- Intense review of liabilities by legal team and Board of Trustees created additional requirements at ARIN XXVI
- Two new big requirements
  - Non-repudiation in ROA generation for hosted CAs
  - Thwart “Evil Mark” (rogue employee) from making changes

General Architecture of RPKI Registration Interface

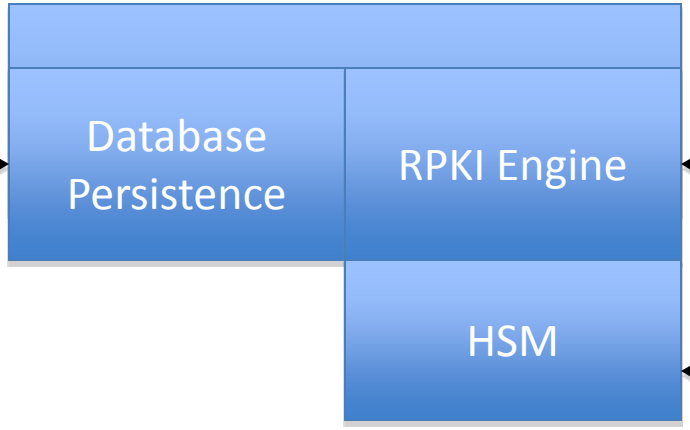


Tight coupling between resource certificate/ROA entities and registration dataset at the database layer. Once certs/ROAs are created, they must be maintained if the registered dependents are changed.

Development before ARIN XXVI

With a few finishing touches, ready to go Jan 1, 2011 with Hosted Model, Delegated Model to follow end of Q1.

Highly influenced by RIPE NCC entities.



RIPE NCC RPKI Engine with a few tweaks.

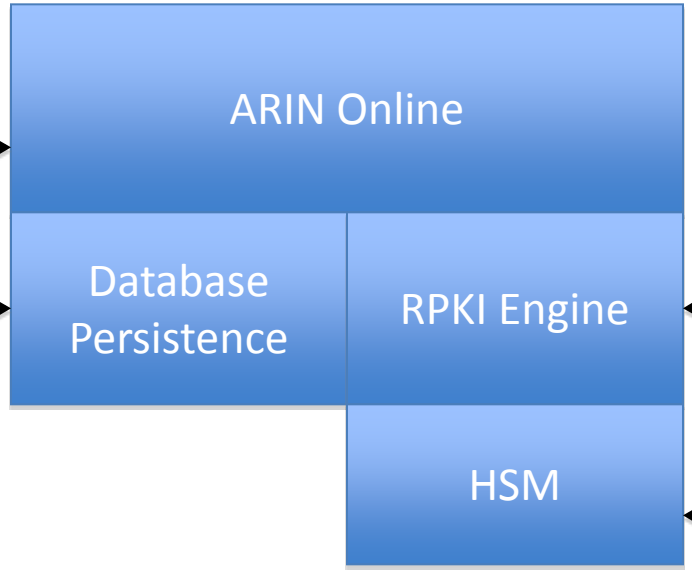
Sun SCA 6000

Everything is Java, JBoss, Hibernate.

Changes Underway Since ARIN XXVI

In-browser ROA request signing via AJAX.

Minor changes.

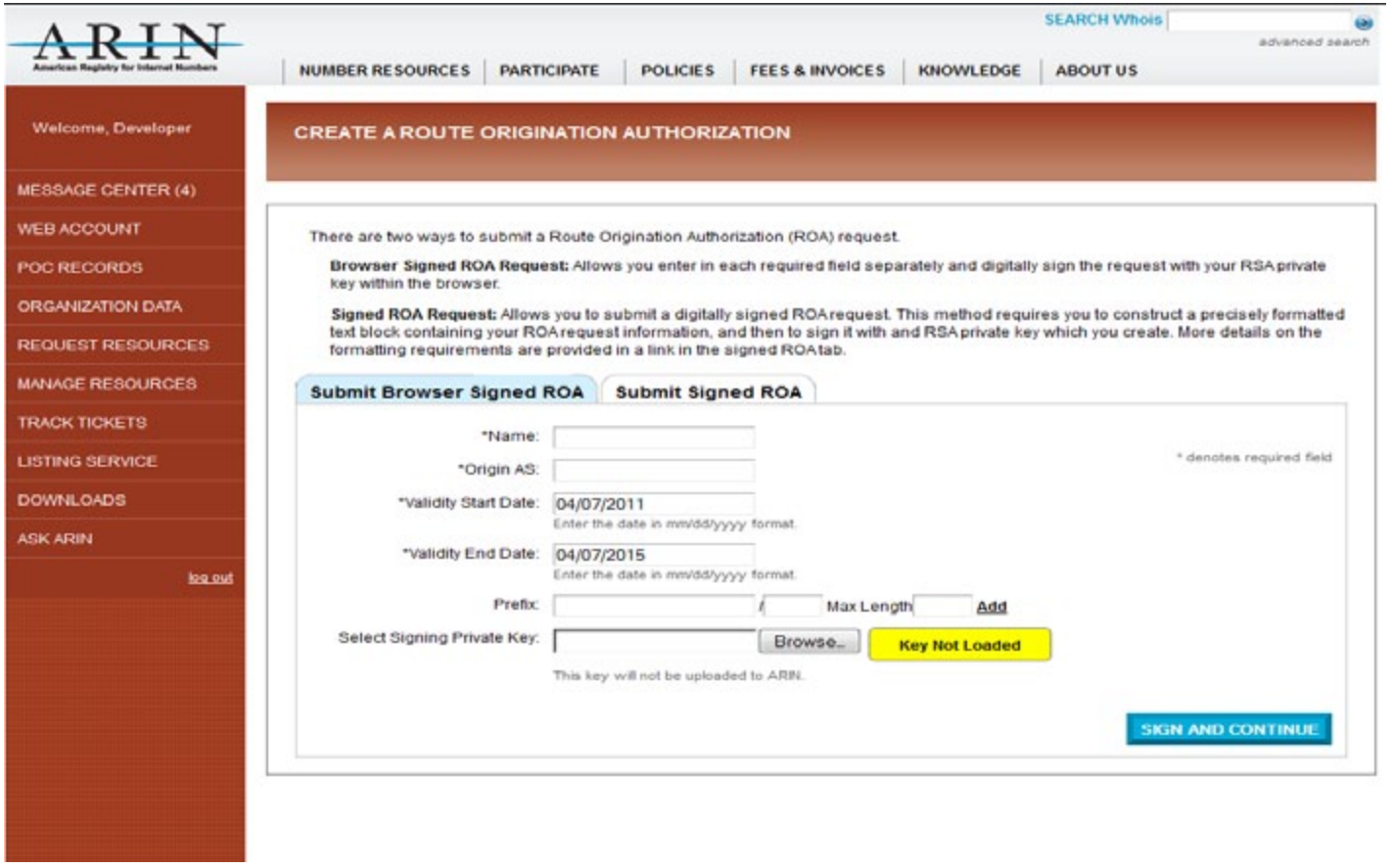


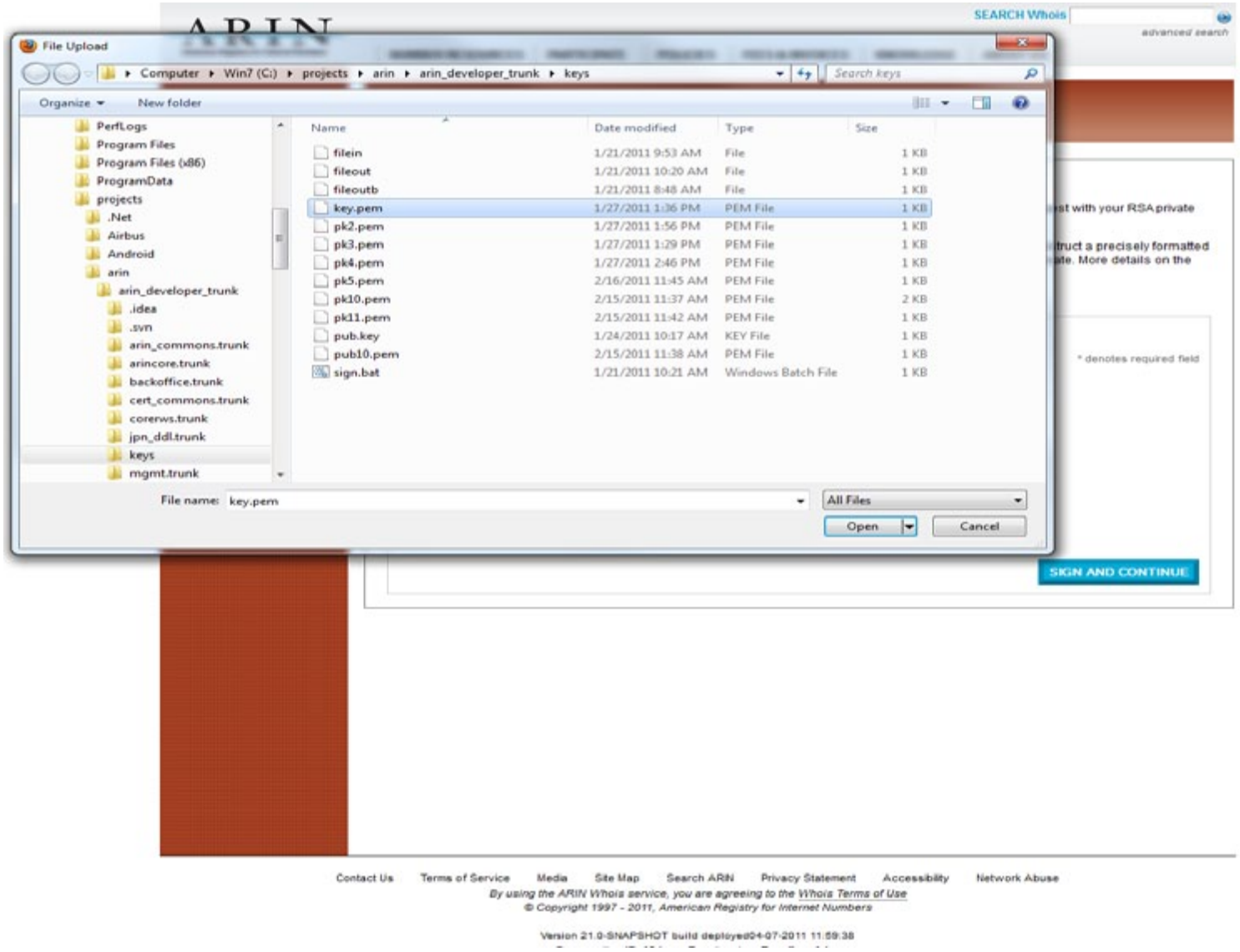
Message driven engine which delegates to the HSM.

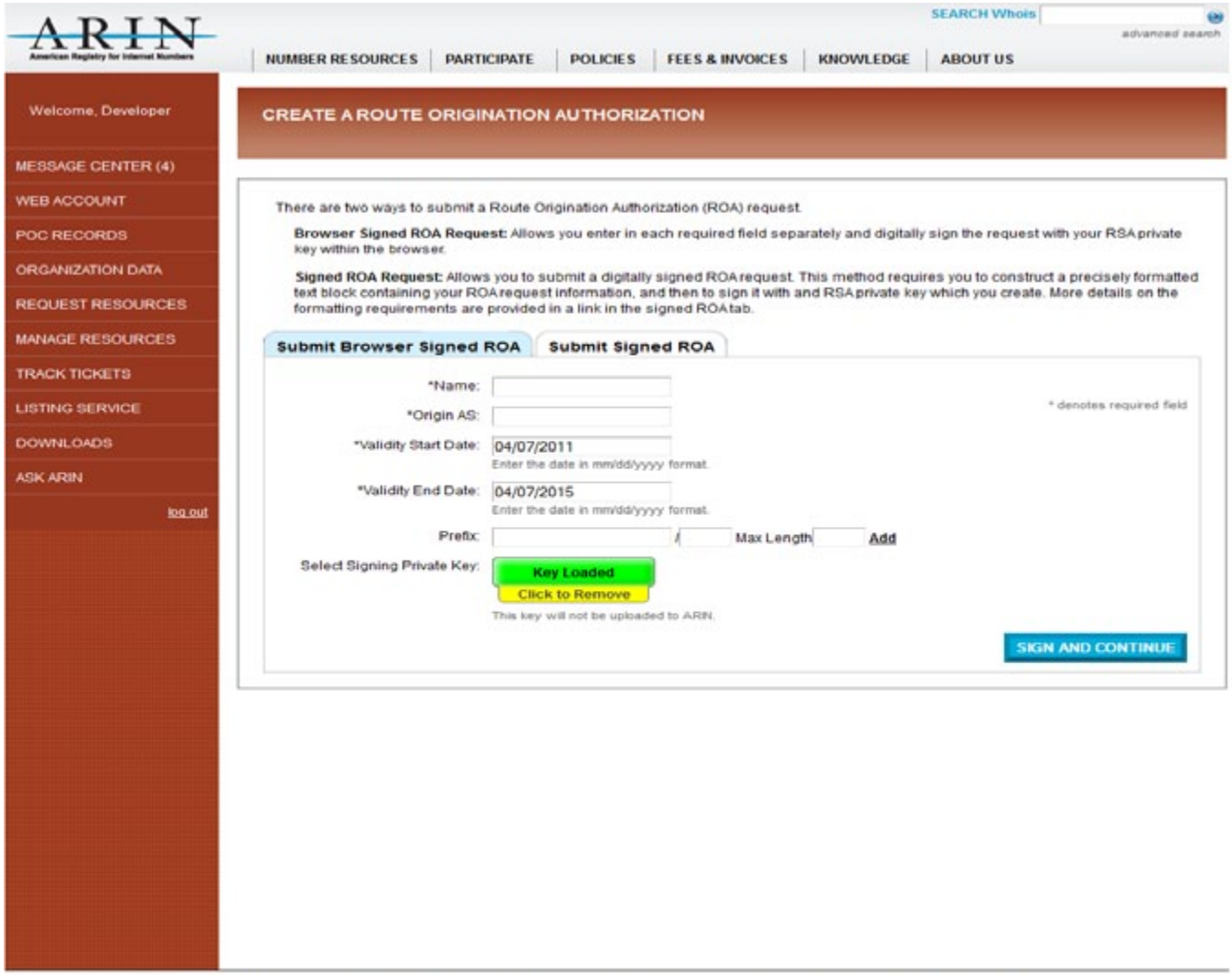
Custom programming on IBM 4764's to enable all DER encoding and crypto.

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

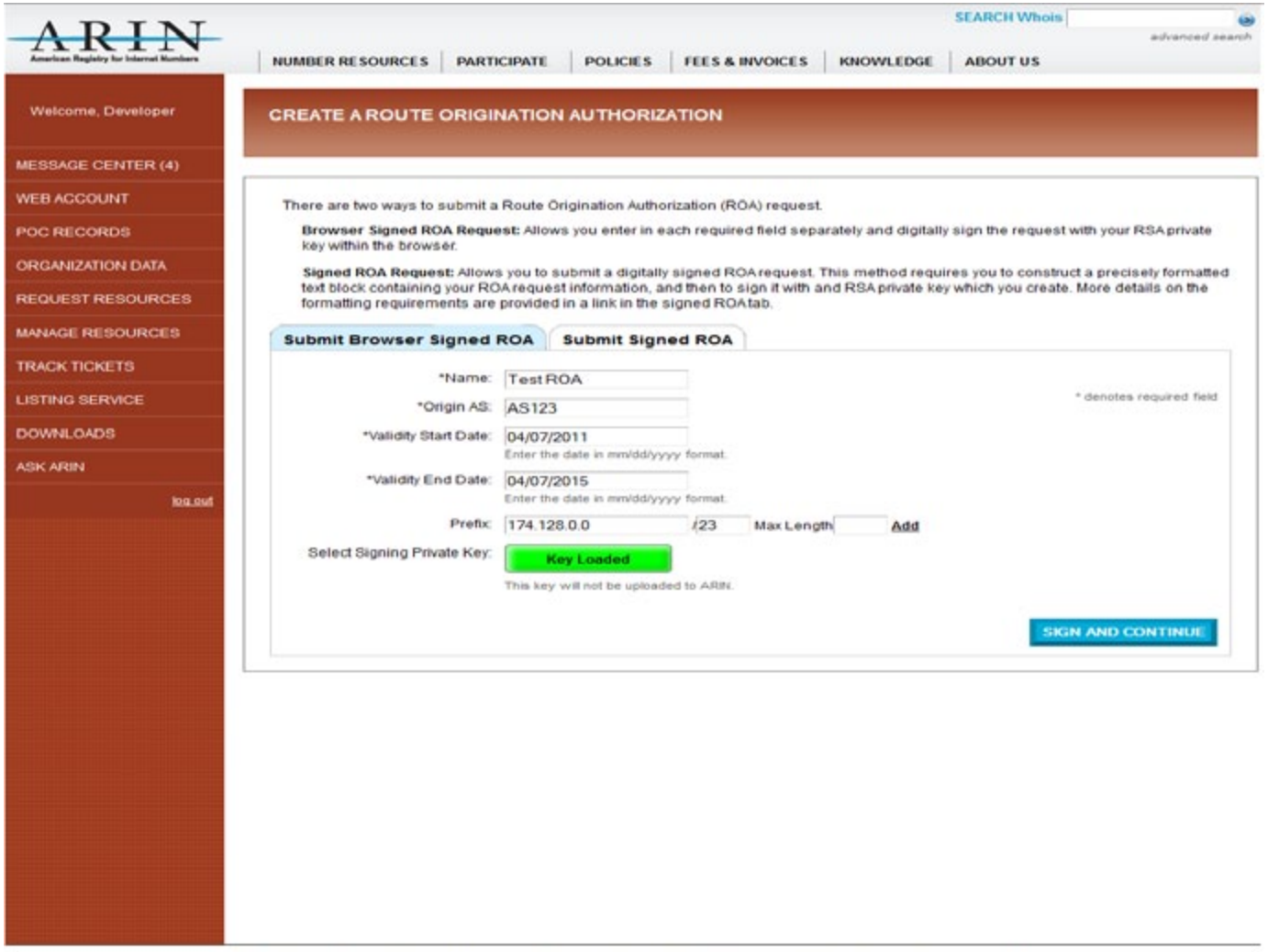
Example – Creating an ROA

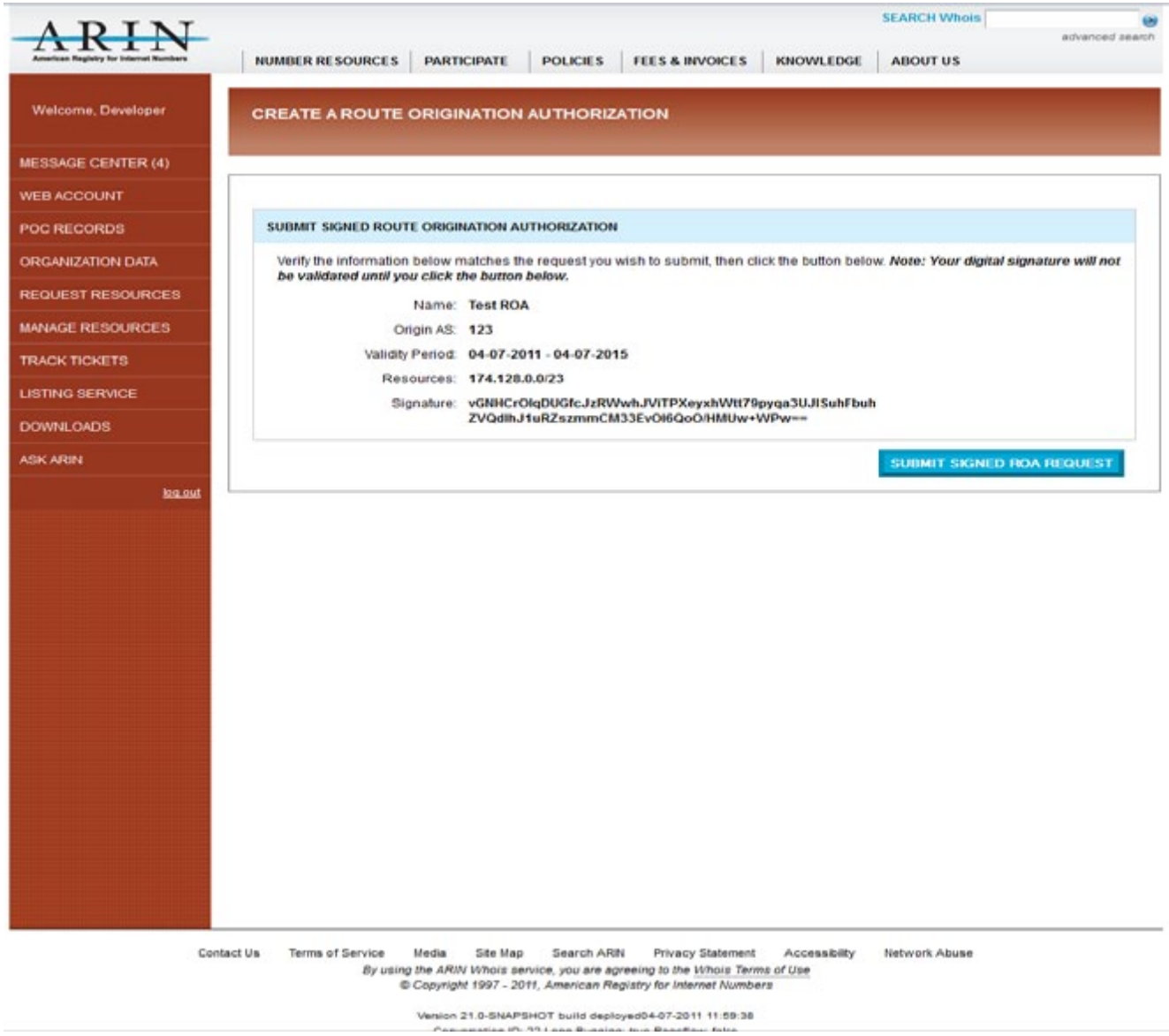


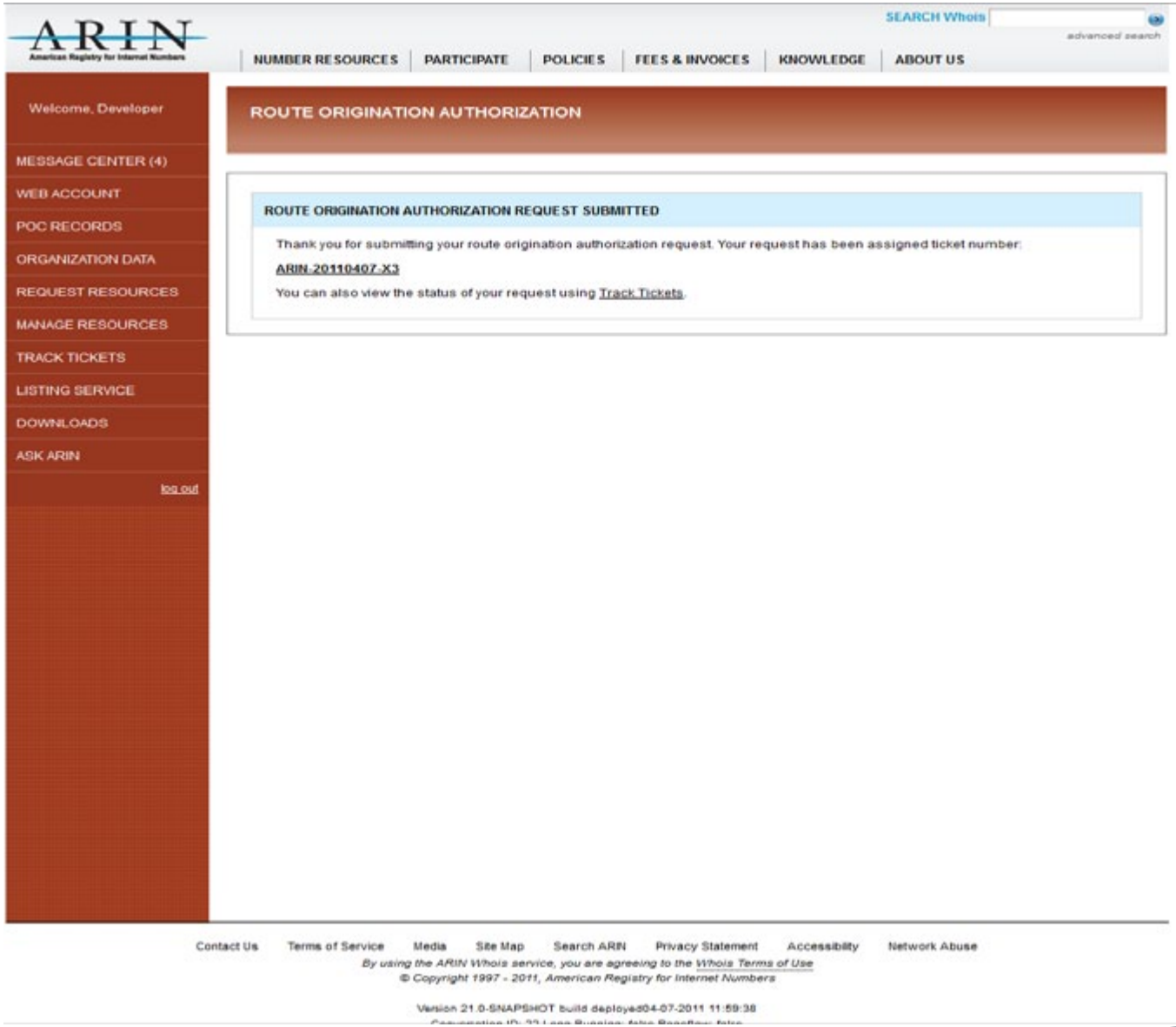

SEARCH Whois
advanced search
File Upload
Computer ▸ Win7 (C:) ▸ projects ▸ arin ▸ arin_developer_trunk ▸ keys
Search keys
Organize
New folder
PerfLogs
Program Files
Program Files (x86)
ProgramData
projects
.Net
Airbus
Android
arin
arin_developer_trunk
.idea
.svn
arin_commons.trunk
arincore.trunk
backoffice.trunk
cert_commons.trunk
corerws.trunk
jpn_ddl.trunk
keys
mgmt.trunk
Name
Date modified
Type
Size
filein 1/21/2011 9:53 AM File 1 KB
fileout 1/21/2011 10:20 AM File 1 KB
fileoutb 1/21/2011 8:48 AM File 1 KB
key.pem 1/27/2011 1:36 PM PEM File 1 KB
pk2.pem 1/27/2011 1:56 PM PEM File 1 KB
pk3.pem 1/27/2011 1:29 PM PEM File 1 KB
pk4.pem 1/27/2011 2:46 PM PEM File 1 KB
pk5.pem 2/16/2011 11:45 AM PEM File 1 KB
pk10.pem 2/15/2011 11:37 AM PEM File 2 KB
pk11.pem 2/15/2011 11:42 AM PEM File 1 KB
pub.key 1/24/2011 10:17 AM KEY File 1 KB
pub10.pem 2/15/2011 11:38 AM PEM File 1 KB
sign.bat 1/21/2011 10:21 AM Windows Batch File 1 KB
File name: key.pem
All Files
Open
Cancel
st with your RSA private
tructa precisely formatted
ate. More details on the
* denotes required field
SIGN AND CONTINUE
Contact Us
Terms of Service
Media
Site Map
Search ARIN
Privacy Statement
Accessibility
Network Abuse
By using the ARIN Whois service, you are agreeing to the Whois Terms of Use
© Copyright 1997 - 2011, American Registry for Internet Numbers
Version 21.0-SNAPSHOT build deployed04-07-2011 11:59:38



ARIN
American Registry for Internet Numbers


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
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: Test ROA
* denotes required field
*Origin AS: AS123
*Validity Start Date: 04/07/2011
Enter the date in mm/dd/yyyy format.
*Validity End Date: 04/07/2015
Enter the date in mm/dd/yyyy format.
Prefix: 174.128.0.0 /23 Max Length Add
Select Signing Private Key: Key Loaded
This key will not be uploaded to ARIN.
SIGN AND CONTINUE
Contact Us
Terms of Service
Media
Site Map
Search ARIN
Privacy Statement
Accessibility
Network Abuse
By using the ARIN Whois service, you are agreeing to the Whois Terms of Use
© Copyright 1997 - 2011, American Registry for Internet Numbers
Version 21.0-SNAPSHOT build deployed04-07-2011 11:59:38


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: vGNHCrOlqDUGfcJzRWwhJViTPXeyxhWtt79pyqa3UJISuhFbuh
ZVQdlhJ1uRZszmmCM33EvOl6QoO/HMUw+WPw==
SUBMIT SIGNED ROA REQUEST
Contact Us
Terms of Service
Media
Site Map
Search ARIN
Privacy Statement
Accessibility
Network Abuse
By using the ARIN Whois service, you are agreeing to the Whois Terms of Use
© Copyright 1997 - 2011, American Registry for Internet Numbers
Version 21.0-SNAPSHOT build deployed04-07-2011 11:59:38


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 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.
Contact Us
Terms of Service
Media
Site Map
Search ARIN
Privacy Statement
Accessibility
Network Abuse
By using the ARIN Whois service, you are agreeing to the Whois Terms of Use
© Copyright 1997 - 2011, American Registry for Internet Numbers
Version 21.0-SNAPSHOT build deployed04-07-2011 11:59:38

Updates within RPKI outside of ARIN

- The four other RIRs are in production with Hosted CA services
- Major routing vendor support being tested
- Announcement of public domain routing code support

ARIN Status

- Hosted CA anticipated next year.

- We intend to add up/down code required for delegated model after Hosted CA completed

Why is this important?

- Provides more credibility to identify resource holders
- Helps in the transfer market identify real resource holders
- Bootstraps routing security

Q&A

ARIN RESTful Web Services

Andy Newton
Chief Engineer

REST – The New Services

- Three RESTful Web Services
  - Whois-RWS
    - Exposes our public Whois data via REST
  - Reg-RWS (or Registration-RWS)
    - Registration and maintenance of your data in a programmatic fashion
  - Bulk Whois
    - Download of Bulk Whois is now down RESTfully

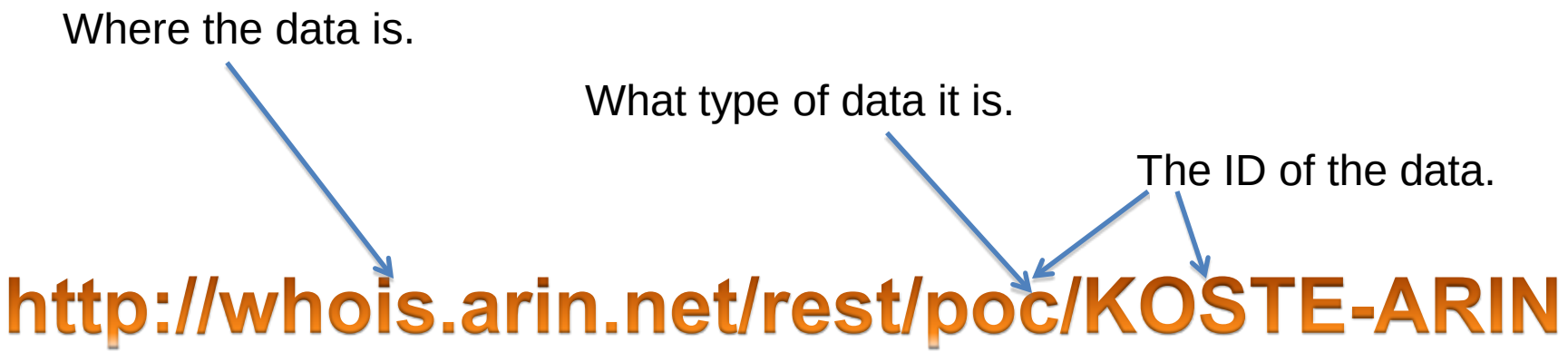
What is REST?

- Representation State Transfer
- As applied to web services
  - defines a pattern of usage with HTTP to create, read, update, and delete (CRUD) data
  - “Resources” are addressable in URLs
- Very popular protocol model
  - Amazon S3, Yahoo & Google services, …

The BIG Advantage of REST

- Easily understood
  - Any modern programmer can incorporate it
  - Can look like web pages
- Re-uses HTTP in a simple manner
  - Many, many clients
  - Other HTTP advantages
- This is why it is very, very popular with Google, Amazon, Yahoo, Twitter, Facebook, YouTube, Flickr, …

What does it look like?
And who can use it?



It is a standard URL.
Go ahead, put it into your browser.

Where can more information on REST be found?

- *RESTful Web Services*
  - O'Reilly Media
  - Leonard Richardson
  - Sam Ruby

Whois-RWS

- Publicly Accessible, just like traditional Whois
- Searches and lookups on IP addresses, AS numbers, POCs, Orgs, etc…
- Very popular
  - As of March, 2011, constitutes 40% of our query load
- For more information:
  - https://www.arin.net/resources/whoisrws/index.html

Reg-RWS

- Requires an API Key
  - You generate one in ARIN Online
- Register and manage your data
  - But only your data
- More information
  - https://www.arin.net/resources/restful-interfaces.html
  - We are working on enhanced documentation – to be released *soonish*

Reg-RWS Has More Than Templates

- Only programmatic way to do IPv6 Reassign Simple
- Only programmatic way to manage Reverse DNS
- Only programmatic way to access you ARIN tickets

Testing Your Reg-RWS Client

- We offer an Operational Test & Evaluation environment for Reg-RWS
- Your real data, but isolated
  - Helps you develop against a real system without the worry that real data could get corrupted.
- For more information:
  - https://www.arin.net/announcements/2011/20110215.html

Bulk Whois

- You must first sign an AUP
  - ARIN staff will review your need to access bulk Whois data
- Also requires an API Key
- More information
  - https://www.arin.net/resources/request/bulkwhois.html

ARIN Provided Libraries

- We will soon have some code you can use
- Reg-RWS Java library
  - Used by ARIN internally
  - Will be released upon completion of documentation
- ARINr
  - Set of Ruby libraries used to prove out our service
  - To be released soon under BSD license
    - “Alpha” quality, seeking community involvement
  - Targets Whois-RWS and Reg-RWS
  - For the command-line oriented power users

Obtaining RESTful Assistance

- ARIN Online's ASK ARIN feature
- arin-tech-discuss mailing list
  - Make sure to subscribe
  - Someone on the list will help you ASAP
- Registration Services Help Desk telephone not a good fit
  - Debugging these problems requires a detailed look at the method, URL, and payload being used

Q&A