Agenda

- DNSSEC
- RPKI
- In-addr.arpa transition
- Directory Service Stats (Whois-RWS)
Changes Required to make DNSSEC work

• Transfer of in-addr.arpa to ICANN
• Signing in-addr.arpa, ip6.arpa and delegations that ARIN manages
• Provisioning of DS Records
  – ARIN Online
  – RESTful Interface (mid-september)
• All completed by 4/27/2011
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 zones listed on the left. If you did not intend to specify a unified set of nameservers for all the reverse DNS zones listed on the left, then please press the CANCEL button to go back to the previous screen.

**SELECTED ZONES IN - NET-64-112-0-0-1**

- 0.112.64.in-addr.arpa.
- 1.112.64.in-addr.arpa.
- 2.112.64.in-addr.arpa.
- 3.112.64.in-addr.arpa.
- 4.112.64.in-addr.arpa.
- 5.112.64.in-addr.arpa.
- 6.112.64.in-addr.arpa.
- 7.112.64.in-addr.arpa.
- 8.112.64.in-addr.arpa.
- 9.112.64.in-addr.arpa.
- 10.112.64.in-addr.arpa.
- 11.112.64.in-addr.arpa.
- 12.112.64.in-addr.arpa.
- 13.112.64.in-addr.arpa.
- 14.112.64.in-addr.arpa.

**HOSTNAMES OF NAMESERVERS**

- Nameserver 1: NS1.WEB-ZERO.NET
- Nameserver 2: NS2.WEB-ZERO.NET
- Nameserver 3: NS3.FOO.COM
- Nameserver 4: NS4.BAR.COM
- Nameserver 5: NS5.BLING.COM
- Nameserver 6:
- Nameserver 7:
- Nameserver 8:
- Nameserver 9:
- Nameserver 10:
- Nameserver 11:
- Nameserver 12:
- Nameserver 13:
RPKI Pilot

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

Everything is Java, JBoss, Hibernate.
From ARIN XXVI

- RPKI Services
  - ARIN to sign (assert) directly assigned/allocated resources
  - Other related services such as storing signatures/assertions for downstreams under review
  - Board of Trustees, along with ARIN General Counsel, are evaluating risks associated with these services
  - ARIN is seeking input from community regarding these services
As a Result...

- Completely new requirements for non-repudiation in ROA generation for hosted CAs
- Completely new requirements to thwart “Evil Mark” (rogue employee)
- Further intense review of liabilities by legal team and Board of Trustees
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

CREATE A ROUTE ORIGINATION AUTHORIZATION

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

Browser Signed ROA Request: Allows you to enter 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 your 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

- Name: 
- Origin AS:  
- 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:  
- Max Length:  

Select Signing Private Key:  
- Browse
- Key Not Loaded

SIGN AND CONTINUE
CREATE A ROUTE ORIGINATION AUTHORIZATION

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

- **Browser Signed ROA Request**: Allows you to enter 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 your 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](https://www.arin.net) ![Submit Signed ROA](https://www.arin.net)

- **Name**: 
- **Origin AS**: 
- **Validly Start Date**: 04/07/2011
- **Validly End Date**: 04/07/2016
- **Prefix**: 
- **Max Length**: 
- **Add**

Select Signing Private Key: 
- **Key Loaded**
- **Click to Remove**

This key will not be uploaded to ARIN.

**SIGN AND CONTINUE**
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:** vGHC0RqjRUGcJz5RMWh/MWTPxuy3H1Y7Pyqga3UJHsufTbuhZVQdihJv Ik3szwncnCM35xQnXU8VwVWPw==

[Submit Signed RRO Request]
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.
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 by end of September at the earliest

• We intend to add up/down code for delegated model by the end of the year
in-addr.arpa Transition

- in-addr.arpa generation moved from ARIN to ICANN on 2/16/11
- in-addr.arpa moved from root servers to RIR/ICANN managed servers
- Servers moved off root in increments from 2/21/11 until 3/7/11
- in-addr.arpa is now signed
- Plan to provision DSs to ICANN for /8’s under ARIN’s control by 5/1/11
- No need for trust anchors by that point
Traffic from a.in-addr-servers.arpa
Whois-RWS Statistics – v6

Cumulative Per month
Whois/Whois-RWS Traffic Loads

- Interesting traffic loads are dissipating
- Now versus 12 months ago
- At ARIN XXV
  - 50% of the queries are self-referential (i.e. source ip 192.168.2.5 asking for 192.168.2.5)
  - Most are singleton queries
  - Was increasing over the last year
  - Started noticing decrease after ARIN XXV
Whois-RWS Traffic Loads

• At ARIN XXVI
  – Saw a rise in traffic day after Google announced OpenID collaboration with Yahoo in September
  – Traffic spiked 300%
  – Top ten sites being login sites for various providers – Yahoo, AOL, and Facebook
  – Approximately 5600 queries per second doing the height of the day
Whois-RWS Statistics - Uptick

Stacked Proxy Total Queries

queries/sec

0.0 1.0 k 2.0 k 3.0 k 4.0 k

Week 34  Week 35  Week 36  Week 37

Whois-RWS Loads

- Loads disappeared soon after ARIN XXVI
- Running “normally” now at 2000 queries per second
Whois-RWS Statistics

Whois Queries

Months

Queries Per Second

[Graph showing the number of Whois queries per second over time, with a significant spike in 2014.]
Cumulative Directory Service Traffic

Months

Queries Per Second

Port 43
Port 80
RESTful
Thank You