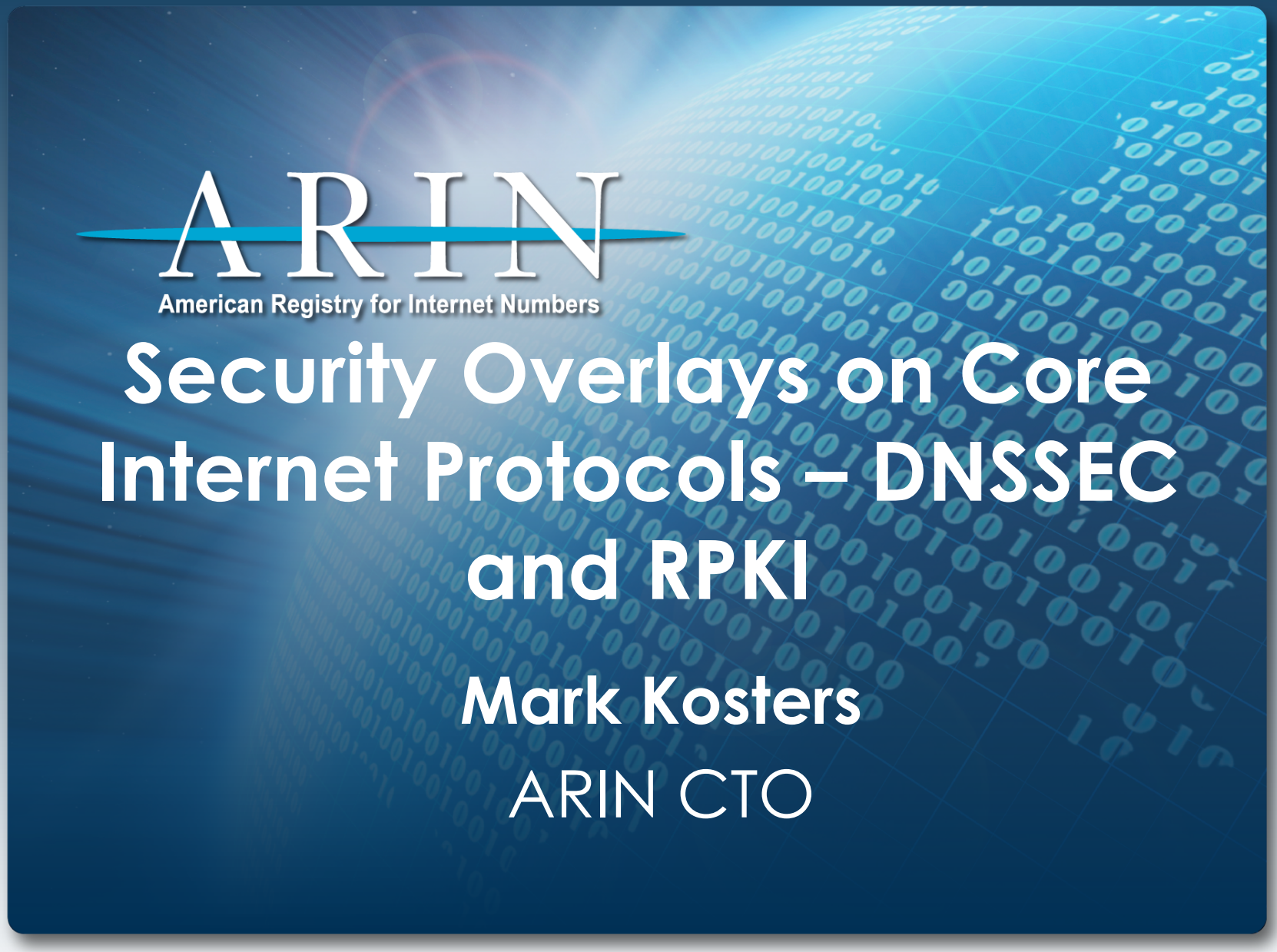



# Security Overlays on Core Internet Protocols – DNSSEC and RPKI

**Mark Kosters**
ARIN CTO

ARIN
American Registry for Internet Numbers

# 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

ARIN
American Registry for Internet Numbers

# 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

ARIN
American Registry for Internet Numbers

# 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

ARIN
American Registry for Internet Numbers

# 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

ARIN
American Registry for Internet Numbers

# 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

ARIN
American Registry for Internet Numbers

# 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…

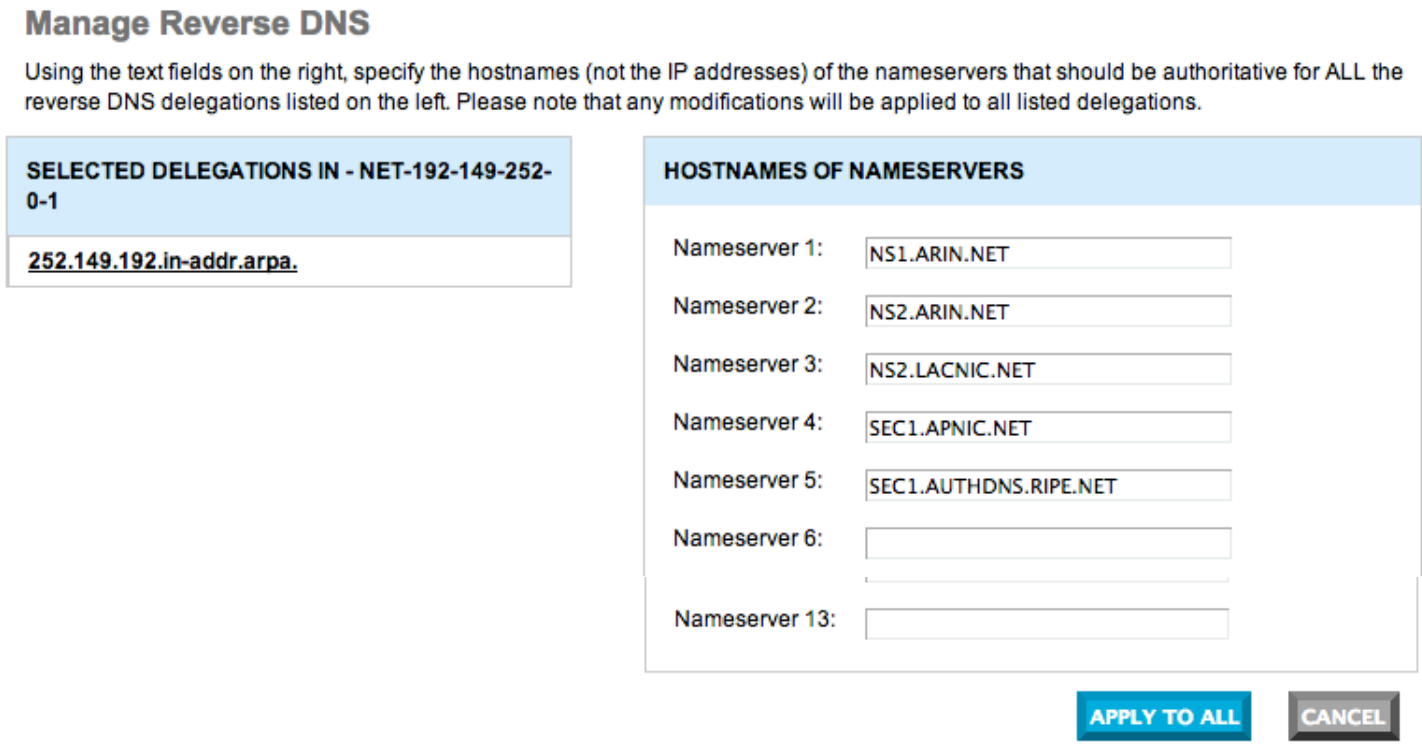
**REVERSE DNS INFORMATION FOR NET-192-149-252-0-1**

| SELECT | DELEGATION | NAMESERVERS | DS RECORD KEY TAGS | AUTHORIZED ORGANIZATIONS |
|---|---|---|---|---|
| ☑ | 252.149.192.in-addr.arpa. | NS1.ARIN.NET<br>NS2.ARIN.NET<br>NS2.LACNIC.NET<br>SEC1.APNIC.NET<br>SEC1.AUTHDNS.RIPE.NET | | ARIN Operations |

MODIFY NAMESERVERS  MODIFY DS RECORDS

# Reverse DNS in ARIN Online

…then enter the Reverse DNS nameservers…



ARIN
American Registry for Internet Numbers

# 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

```
; File written on Mon Feb 24 17:00:53 2014
; dnssec_signzone version 9.3.6-P1-RedHat-9.3.6-20.P1.el5_8.6
0.74.in-addr.arpa.      86400   IN NS   NS3.COVAD.COM.
                        86400   IN NS   NS4.COVAD.COM.
                        10800   NSEC    1.74.in-addr.arpa. NS RRSIG NSEC
                        10800   RRSIG   NSEC 5 4 10800 20140306210053 (
                                        20140224210053 57974 74.in-addr.arpa.
                                        oNk3GVaCWj2j8+EAr0PncqnZeQjm8h4w51nS
                                        D2VUi7YtR9FvYLF/j4KO+8qYZ3TAixb9c05c
                                        8EVIhtY1grXEdOm30zJpZyaoaODpbHt8FdWY
                                        vwup9Tq4oVbxVyuSNXriZ2Mq55IIMgDR3nAT
                                        BLP5UClxUWkgvS/6poF+W/1H4QY= )
1.74.in-addr.arpa.      86400   IN NS   NS3.COVAD.COM.
                        86400   IN NS   NS4.COVAD.COM.
                        10800   NSEC    10.74.in-addr.arpa. NS RRSIG NSEC
                        10800   RRSIG   NSEC 5 4 10800 20140306210053 (
                                        20140224210053 57974 74.in-addr.arpa.
                                        DKYGzSDtIypDVcer5e+XuwoDW4auKy6G/OCV
                                        VTcfQGk+3iyy2CEKOZuMZXFaaDvXnaxey9R1
                                        mjams519Ghxp2qOnnkOw6iB6mR5cNkYlkL0h
                                        lu+IC4Buh6DqM4HbJCZcMXKEtWE0a6dMf+tH
                                        sa+5OV7ezX5LCuDvQVp6p0LftAE= )
```

# 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+sbzQN4LmHzlOi0C/hkaSVO3q1y
                                          6J0KjqNPzYqtxLgZjU+IL9qhtIOocgNQib9l
                                          gFRmZ9inf2bER435GMsa/nnjpVVWW/MBRKxf
                                          Pcc72w2iOAMu2G0prtVT08ENxtu/pBfnsOZK
                                          nhCY8UOBOYLOLE5Whtk3XOuX9+U= )
                         10800   NSEC     1.121.74.in-addr.arpa. NS DS RRSIG
NSEC
                         10800   RRSIG    NSEC 5 5 10800 20140306210053 (
                                          20140224210053 57974 74.in-addr.arpa.
                                          YvRowkdVDfv+PW42ySNUwW8S8jRyV6EKKRxe
…
```

ARIN
American Registry for Internet Numbers

# 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/

ARIN
American Registry for Internet Numbers

# 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

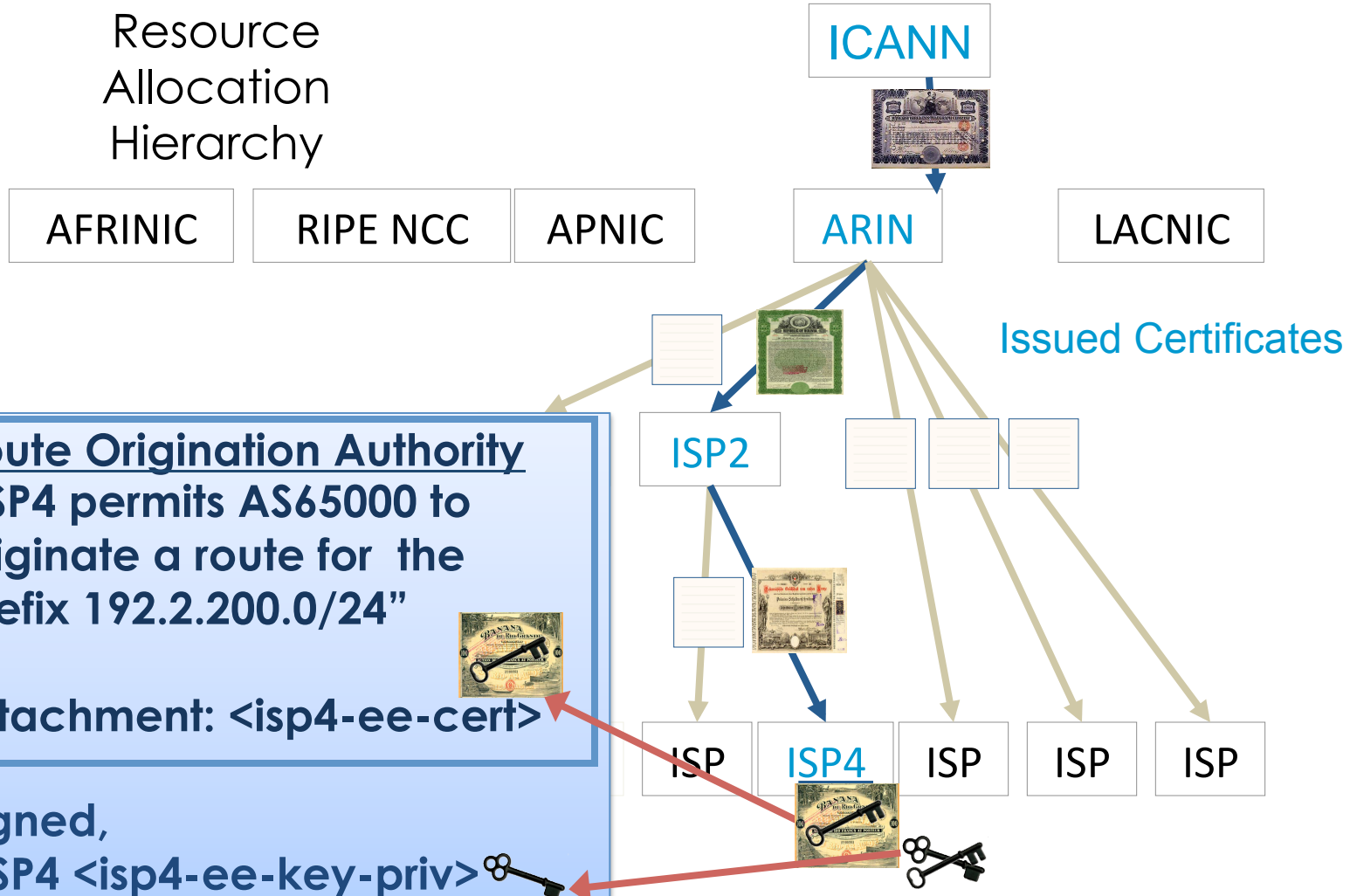
ARIN
American Registry for Internet Numbers

# 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




**Route Origination Authority**

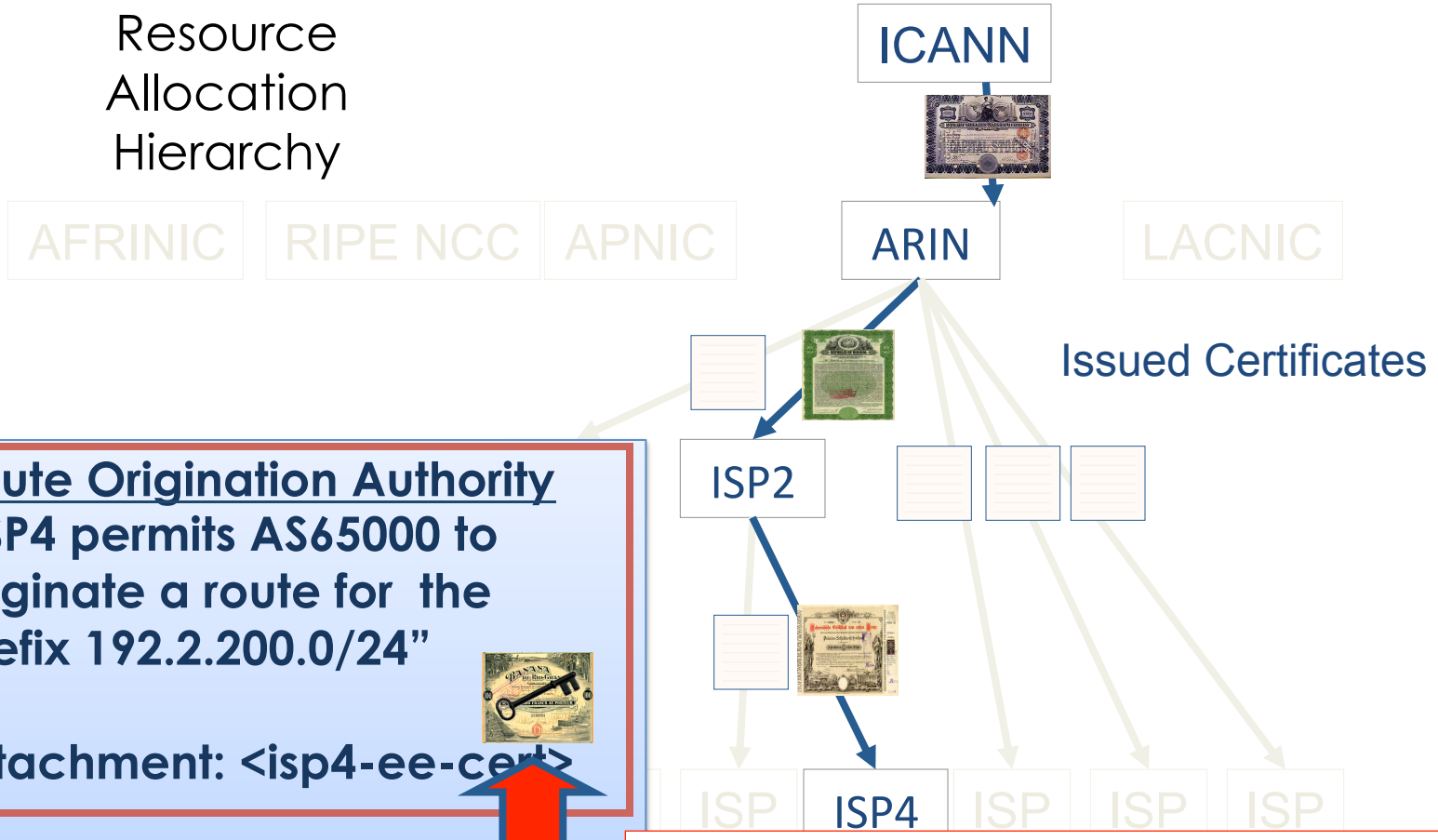
**"ISP4 permits AS65000 to originate a route for the prefix 192.2.200.0/24"**

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

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

# Resource Cert Validation

Resource Allocation Hierarchy




**Route Origination Authority**

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

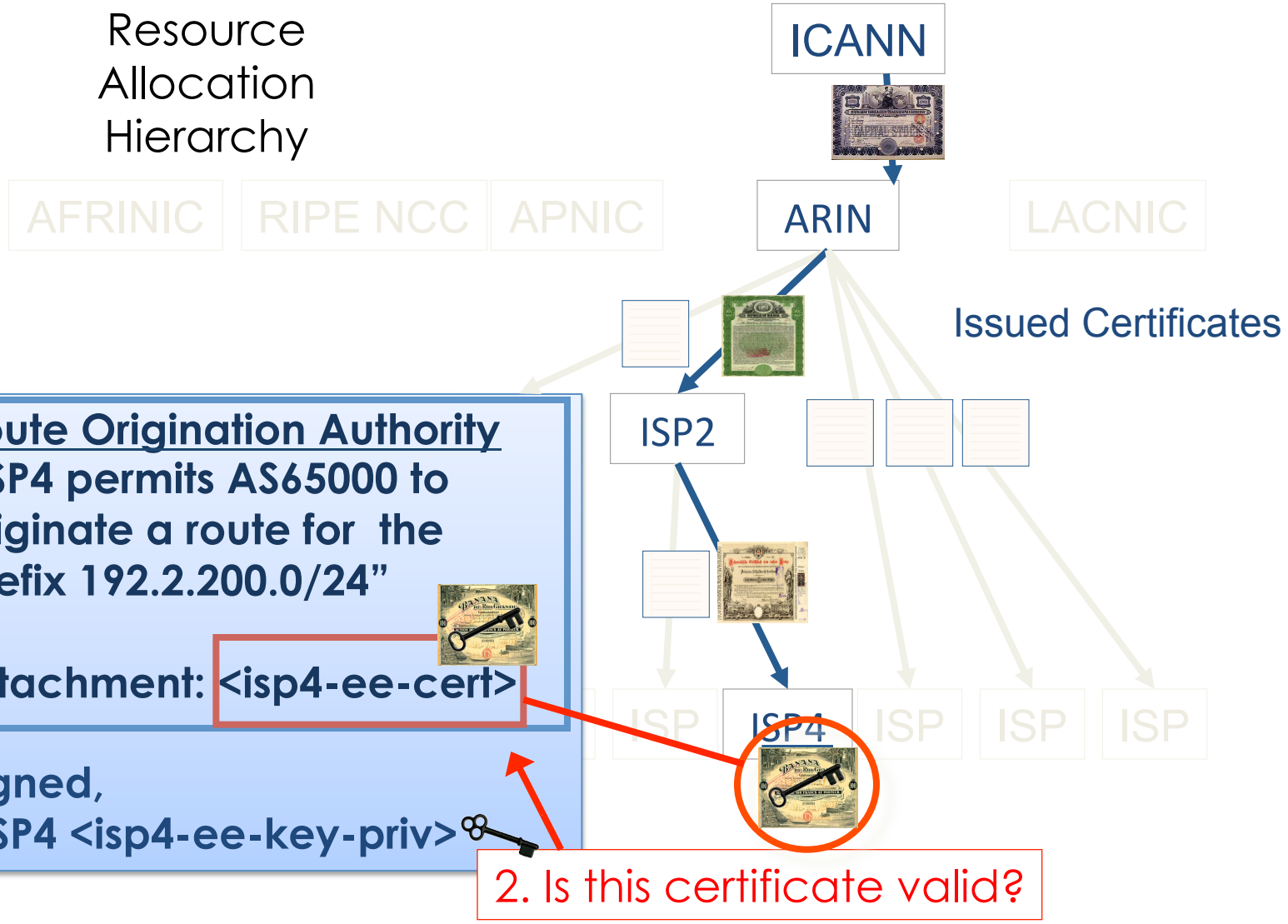
**Attachment: <isp4-ee-cert>**

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

1. Did the matching private key sign this text?

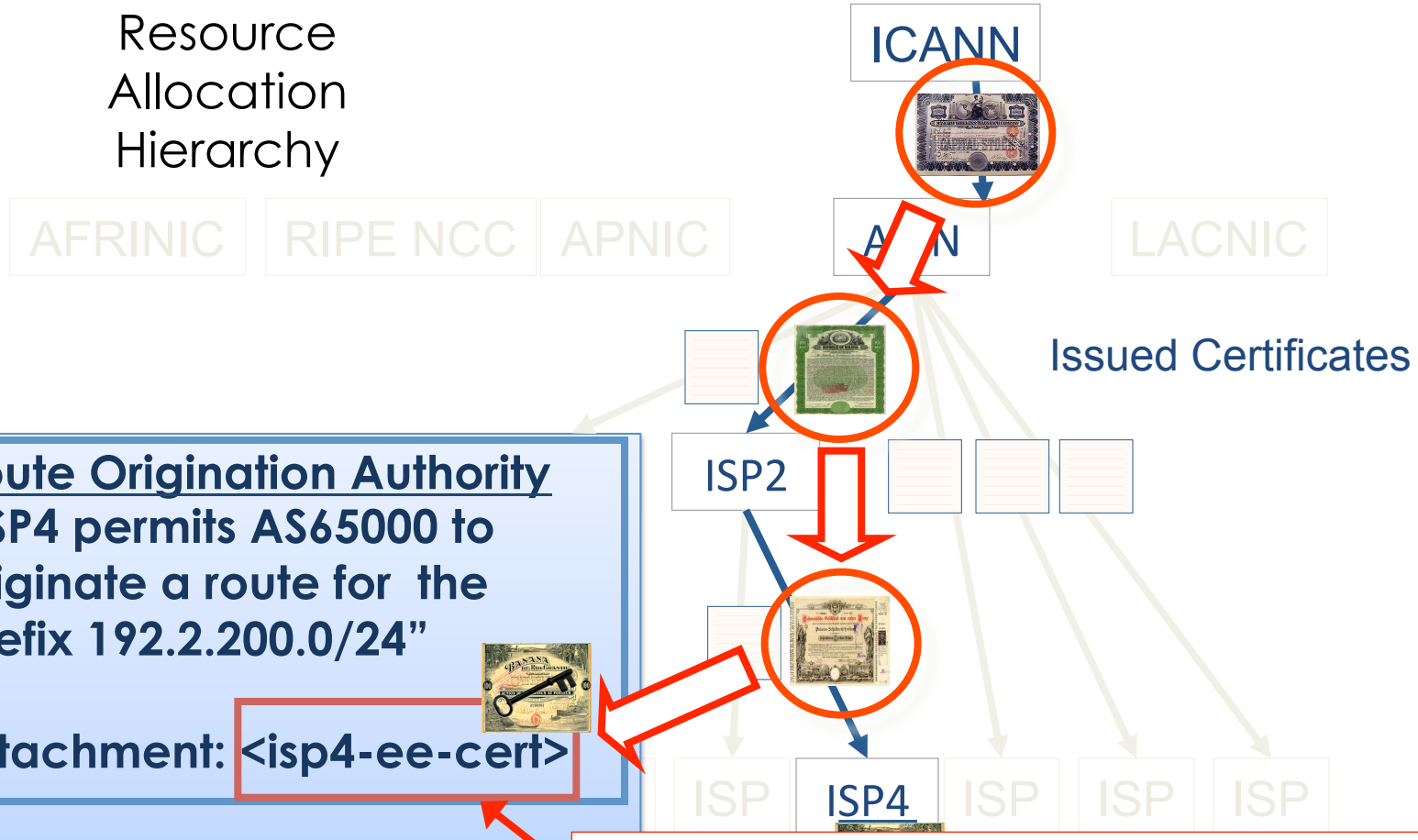
# Resource Cert Validation

Resource Allocation Hierarchy



# 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>**

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

ARIN
American Registry for Internet Numbers

# 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

ARIN
American Registry for Internet Numbers

# 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

ARIN
American Registry for Internet Numbers

# Possible Flow

- RPKI Web interface -> Repository
- Repository aggregator -> Validator
- Validated entries -> Route Checking
- Route checking results -> local routing decisions (based on local policy)

ARIN
American Registry for Internet Numbers

# How you can use ARIN's RPKI System?

- Hosted
- Hosted using ARIN's RESTful service
- Web Delegated (being deprecated)
- Delegated using Up/Down Protocol

ARIN
American Registry for Internet Numbers

# 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

ARIN
American Registry for Internet Numbers

# Hosted RPKI with RESTful Interace

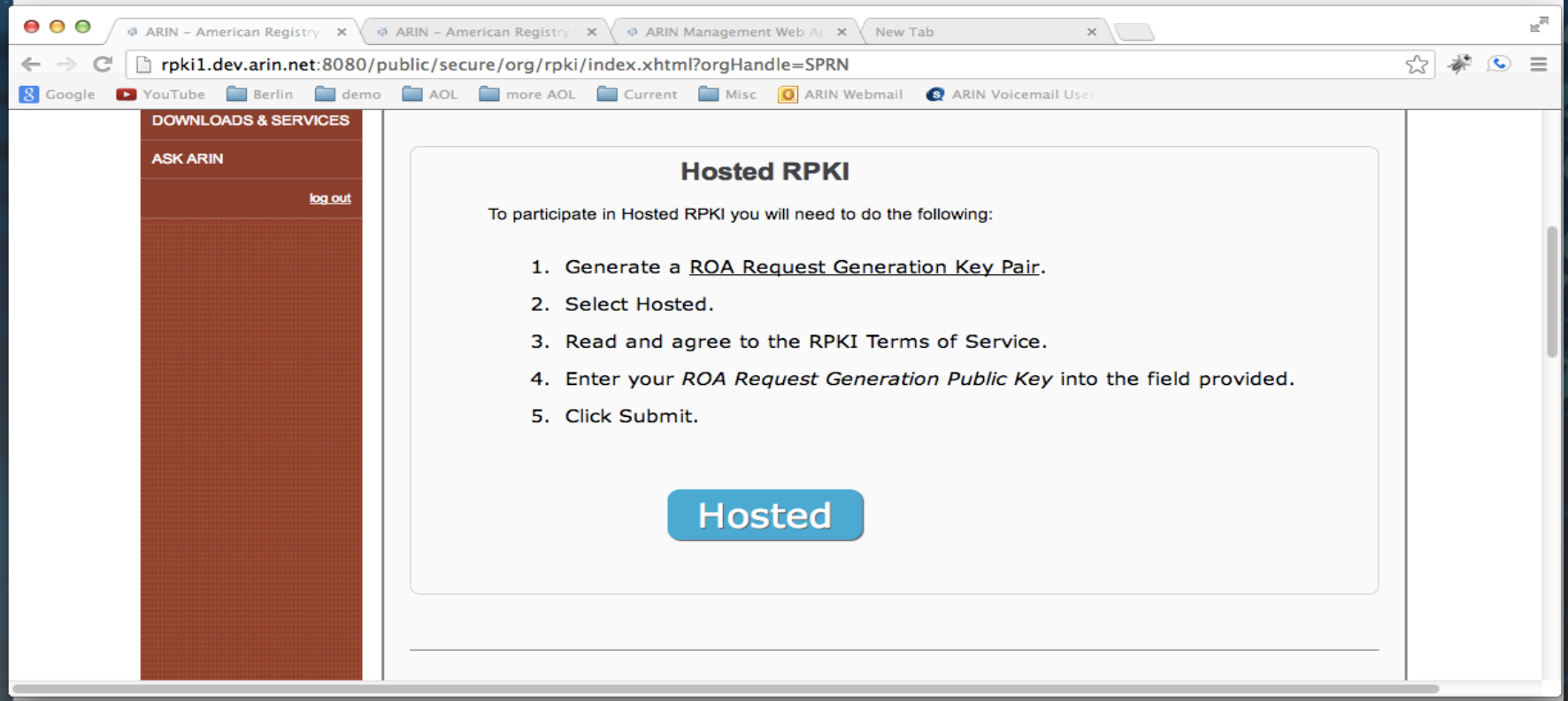
- Pros
  - Easier to use
  - ARIN managed
  - Programmatic interface for large networks
- Cons
  - No current support for downstream customers to manage their own space (yet)
  - We hold your private key

ARIN
American Registry for Internet Numbers

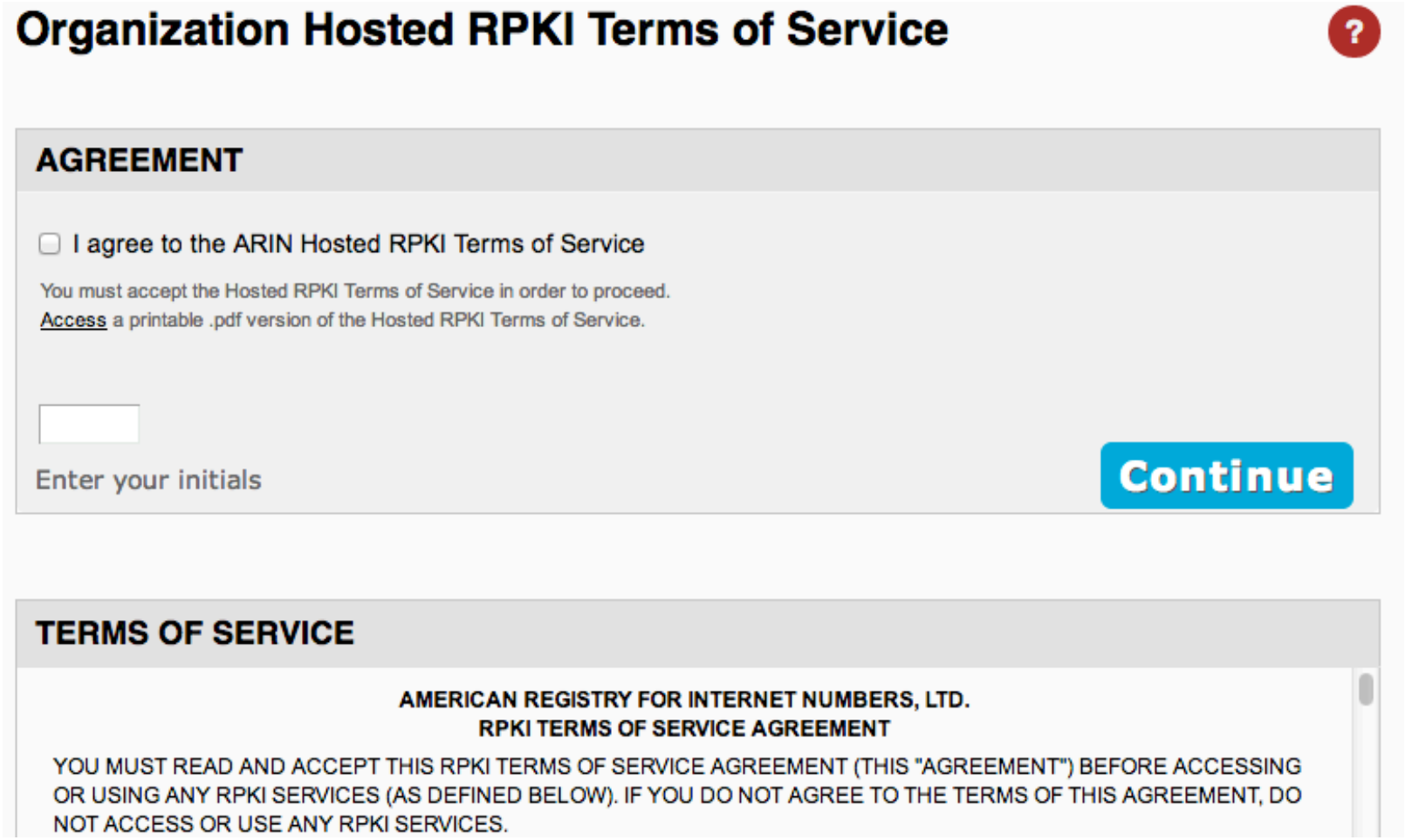
# Delegated RPKI with Up/Down

- 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



ARIN
American Registry for Internet Numbers

# 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/6SHORJGCtuoMUS6tVamIqgdTZJw+8POFku+WlOLgUJOEw763rQVTsAq8WZ
vs6px2FNr6CJftKAr3fg/T083vHYiMtYJnJbVPKJjdSQSylyUWleR2hYh/4LEOyK
MPr3zAuDS2QOI6778OY/kpTEsCrwzp+dM4KtLGOQbyrkfSVlHgux5pCMzsQP/8nP
son5vOlkWtkuFNmg8pXgLfEdBR6MC0Y7eKaTeYM6EEJ7rhUCY69SUq+SFmuwYFsg
7YNzRAErF9THpEWqOaOxaSu/4nwLVJ2oexksT6k4hsEWPadxJ0P3E0FHSb/YlfOS
fwIDAQAB
-----END PUBLIC KEY-----
```

Submit

ARIN
American Registry for Internet Numbers

# 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.

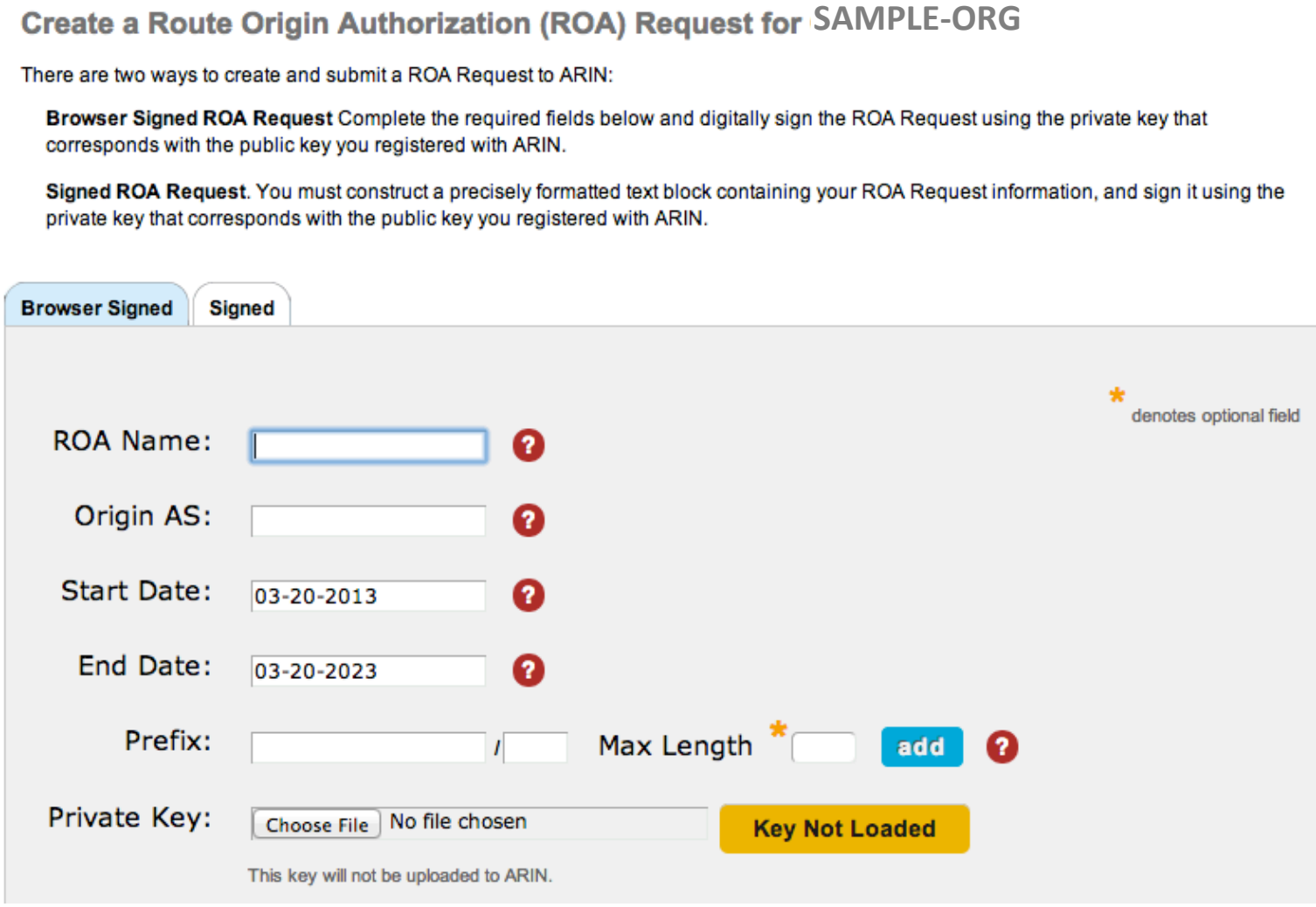
For more information about resource certificates, visit ARIN's RPKI section.

**ARIN** *Updated: 03-20-2013*

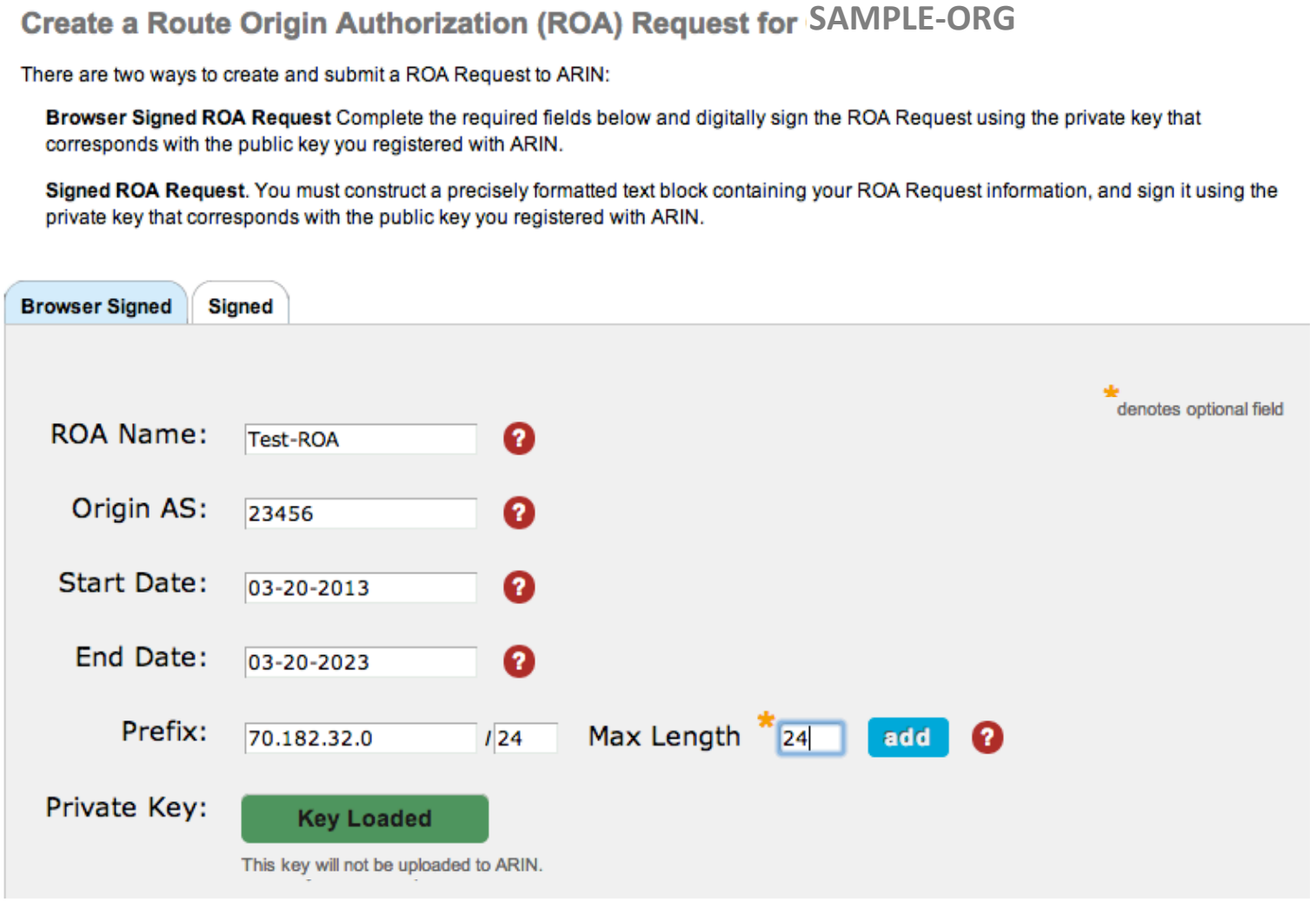
**ROAs:** 0 **Nets:** 20 **ASNs:** 10

Create Roa | View Resources | View Roas | View Details

# Hosted RPKI in ARIN Online



# Hosted RPKI in ARIN Online



ARIN
American Registry for Internet Numbers

# Hosted RPKI in ARIN Online

**SUBMIT SIGNED ROUTE ORIGIN AUTHORIZATION**

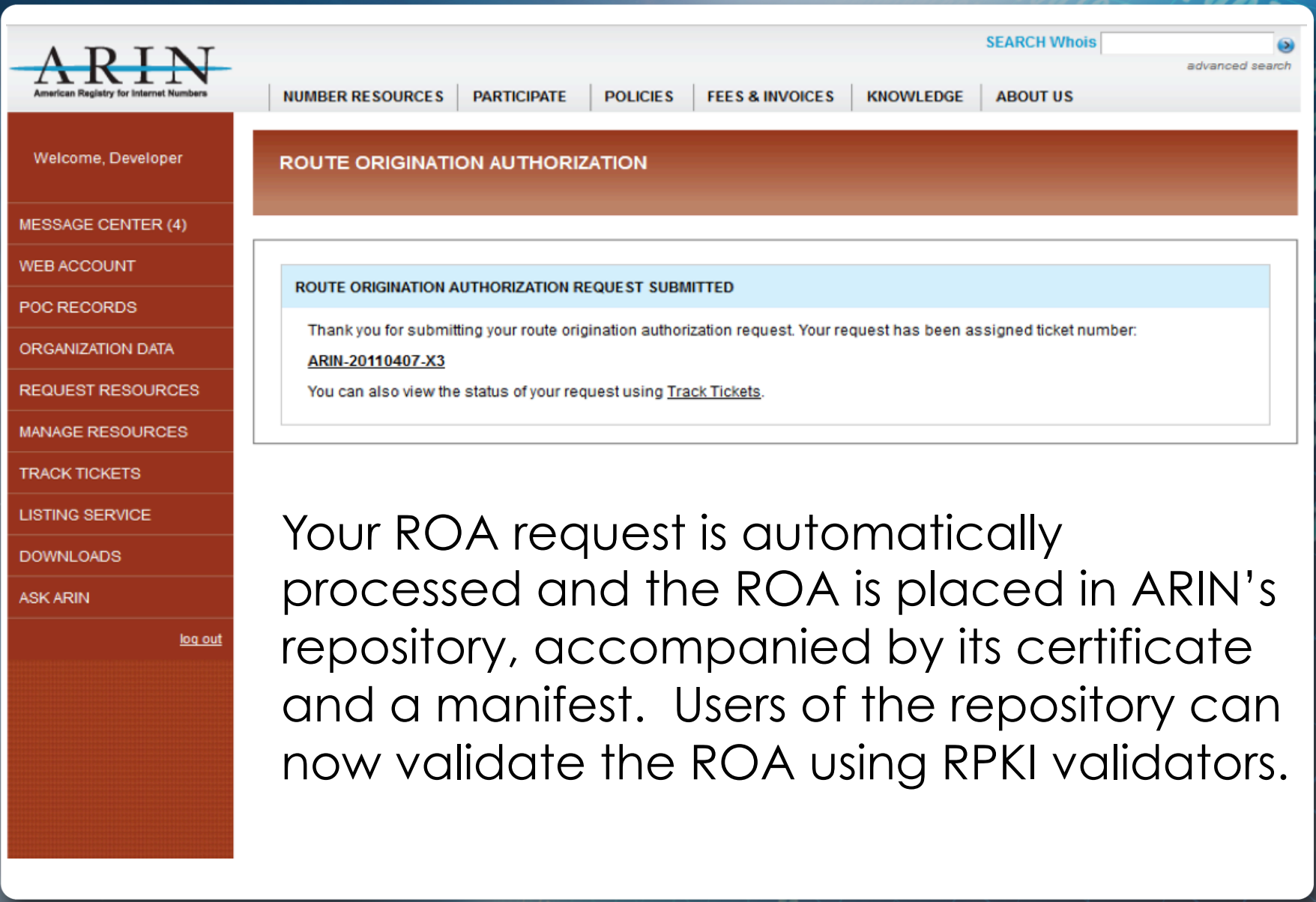
This information will not be saved until you click the **Submit** button below. Note that the signature is used by ARIN to ensure that the ROA Request was signed with your private key. Please verify that the information below is correct. Click **Submit** to send the request, or click **Back** to make 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+JElSgauVyy2htnAPI5rI1Z GY42Fb9c1CEoE8GmT/FWY+CX6UmKsxJ8LQ0NGR2XUeGKZyc2k5 gKiSCog976VnItt88/z5jOm1GkYQoQvk6uyy+yYUKreC+GyNqP YyPAvGAq61jYIDXMhDTSjWdGRiV2dNQ8zMmoDOgm9A==** |

BACK

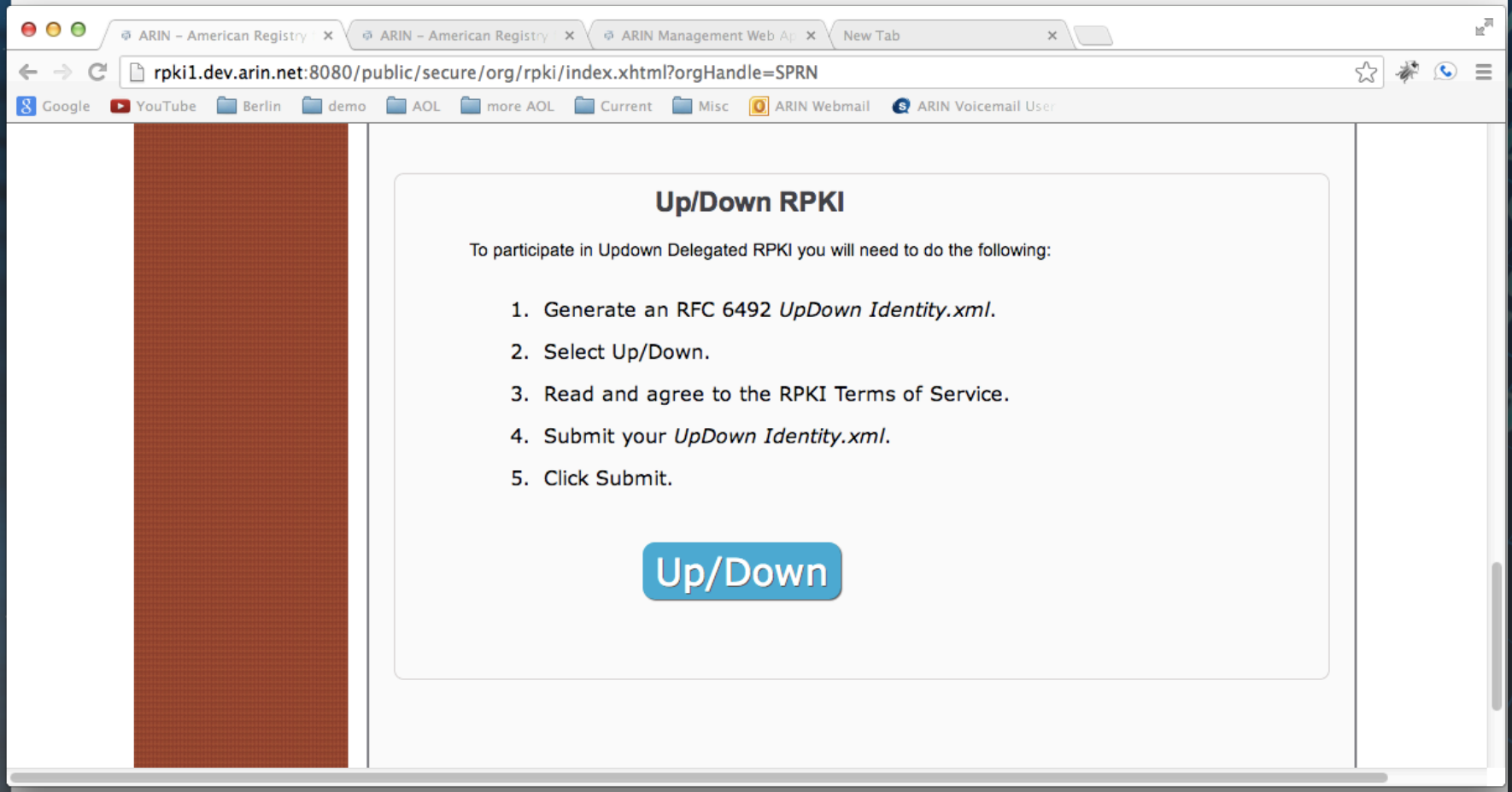
Submit Signed ROA Request

ARIN
American Registry for Internet Numbers

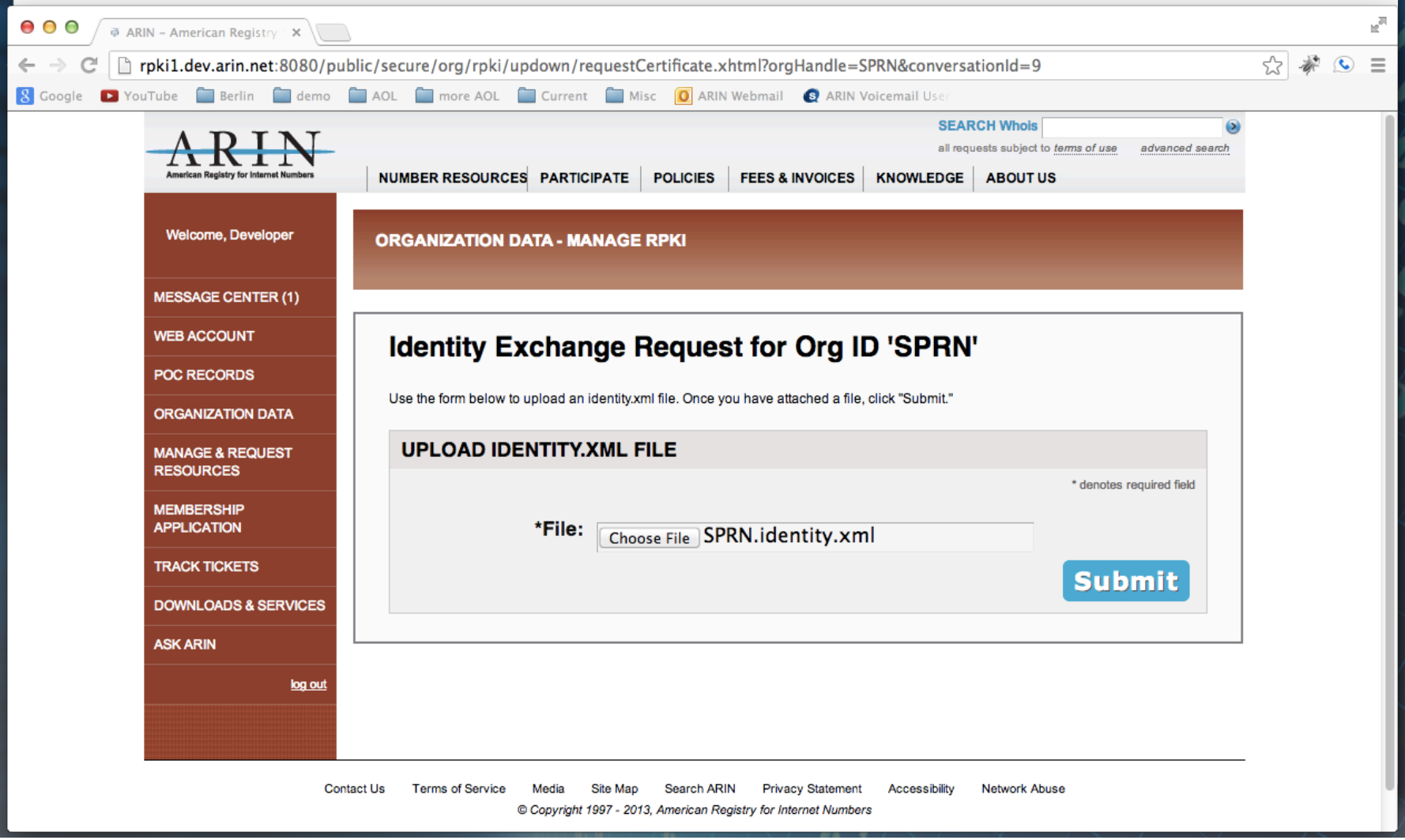



Your ROA request is automatically processed and the ROA is placed in ARIN's repository, accompanied by its certificate and a manifest. Users of the repository can now validate the ROA using RPKI validators.

# Delegated with Up/Down

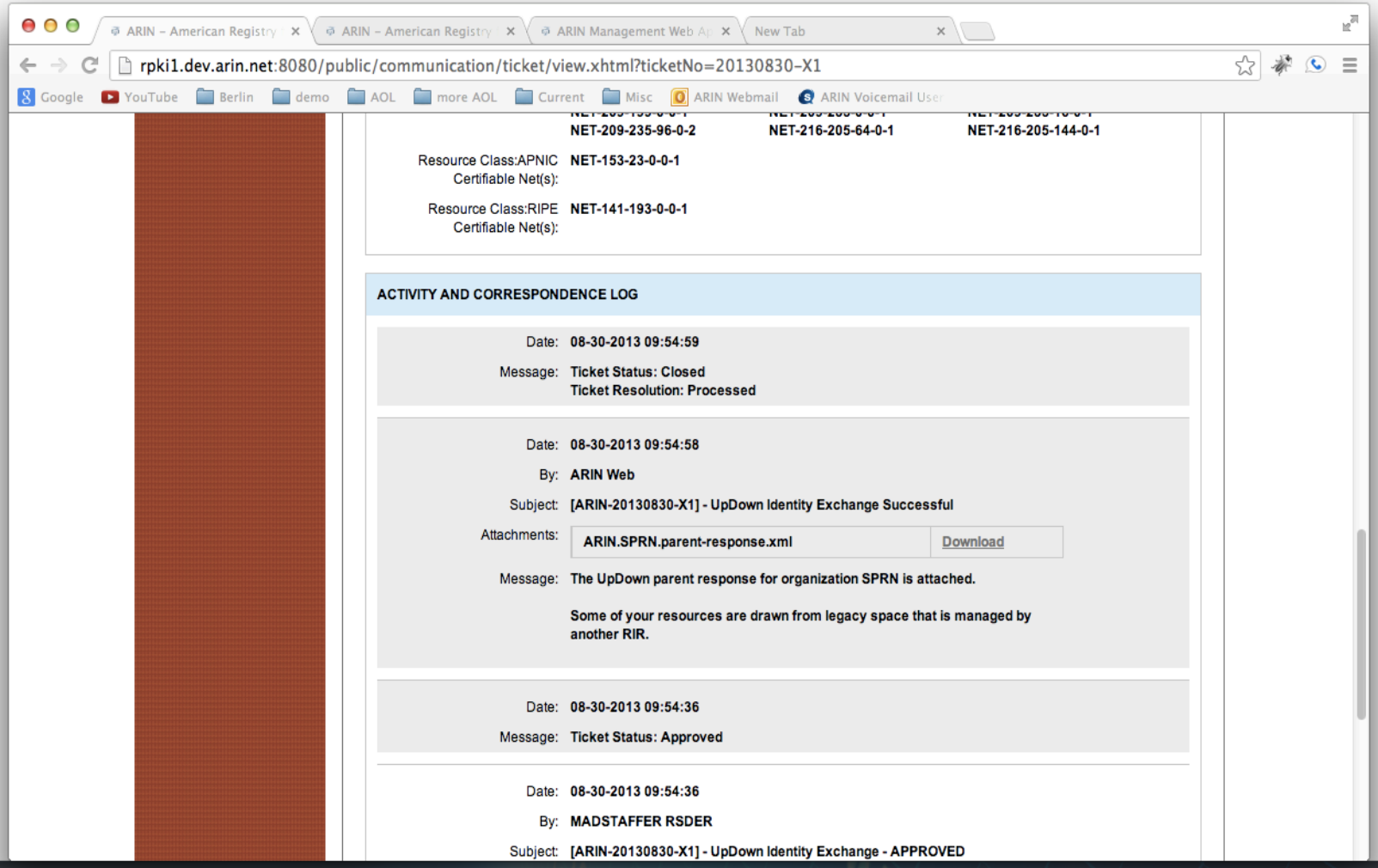


# Delegated with Up/Down



ARIN
American Registry for Internet Numbers

# Delegated with Up/Down



ARIN
American Registry for Internet Numbers

# 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

ARIN
American Registry for Internet Numbers

# 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
American Registry for Internet Numbers

# 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

ARIN
American Registry for Internet Numbers

# RPKI Usage

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

ARIN
American Registry for Internet Numbers

# Why is this important?

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

ARIN
American Registry for Internet Numbers

# Q&A