Practical BGP Origin Validation using RPKI

Moderators:

- Doug Montgomery (dougm@nist.gov)
  NIST
- Sandra Murphy (sandy@tislabs.com)
  Parsons

Track Agenda

- RPKI Introduction
  - Doug Montgomery/NIST, Sandra Murphy/PARSONS
- ARIN RPKI Services
  - Mark Kosters / ARIN – Users' guide to ARIN RPKI services.
- RPKI Implementations
  - Doug / Sandy – Quick survey of RPKI software components.
- Router Vendor Implementations
  - Keyur Patel & Arjun Sreekantiah/Cisco, John Scudder/Juniper, Greg Hankins/ Nokia
- RPKI Test, Training, Monitoring, Management, tools.
  - Matthias Wählisch/FU Berlin, Doug Montgomery, Sandy Murphy
- Deployment Experiences Panel
  - JR Mayberry/Microsoft, Tony Tauber/Comcast, Thomas King/ DE-CIX Henk Steenman/AMS-IX

The Need for BGP Origin Validation

- Malicious BGP route hijacks and accidental misoriginations threaten the security and robustness of the global Internet.
  - ***Invisible Hijacking: A case study of hijacking millions of IP address invisibly.***
    - https://ripe72.ripe.net/presentations/45-Invisible_Hijacking.pdf
  - ***Large Hijack Affects Reachability of High Traffic Destinations***
    - http://www.bgpmon.net/large-hijack-affects-reachability-of-high-traffic-destinations/
  - ***Breaking HTTPS with BGP Hijacking***
    - https://www.blackhat.com/docs/us-15/materials/us-15-Gavrichenkov-Breaking-HTTPS-With-BGP-Hijacking-wp.pdf
  - ***BGP Hijacking for Cryptocurrency Profit***
    - https://www.secureworks.com/research/bgp-hijacking-for-cryptocurrency-profit
- The incidents, methods and motives continue to evolve, the systemic problem remains the same.
  - See: https://securerouting.net/incident

BGP Origin Validation Using RPKI

- Resource Public Key Infrastructure (RPKI)
  - Over the last several years the IETF, RIRs, router vendors, and researchers have developed and implemented an approach to BGP origin validation based upon a global resource public key infrastructure (RPKI).
  - Address owners digitally sign **Route Origin Authorizations (ROAs)** to specify the ASN(s) authorized to announce their prefixes.
  - The approach that permits operators anywhere in the Internet to detect unauthorized route originations and implement local polices to mitigate (e.g., filter) these events.
- This track will examine the current state of RPKI Origin Validation (ROV) technologies, services, products and operational experience.

Two Sides of Using RPKI

- **Certification (Securing routes to your addresses)**
  - Get certificates for your address space
  - Sign ROAs
  - Maintain a CA repository
  - Create certificates for your customers
    - If you give them addresses
- *Think of this as signing the back of your credit card*
- *or registering a route object*

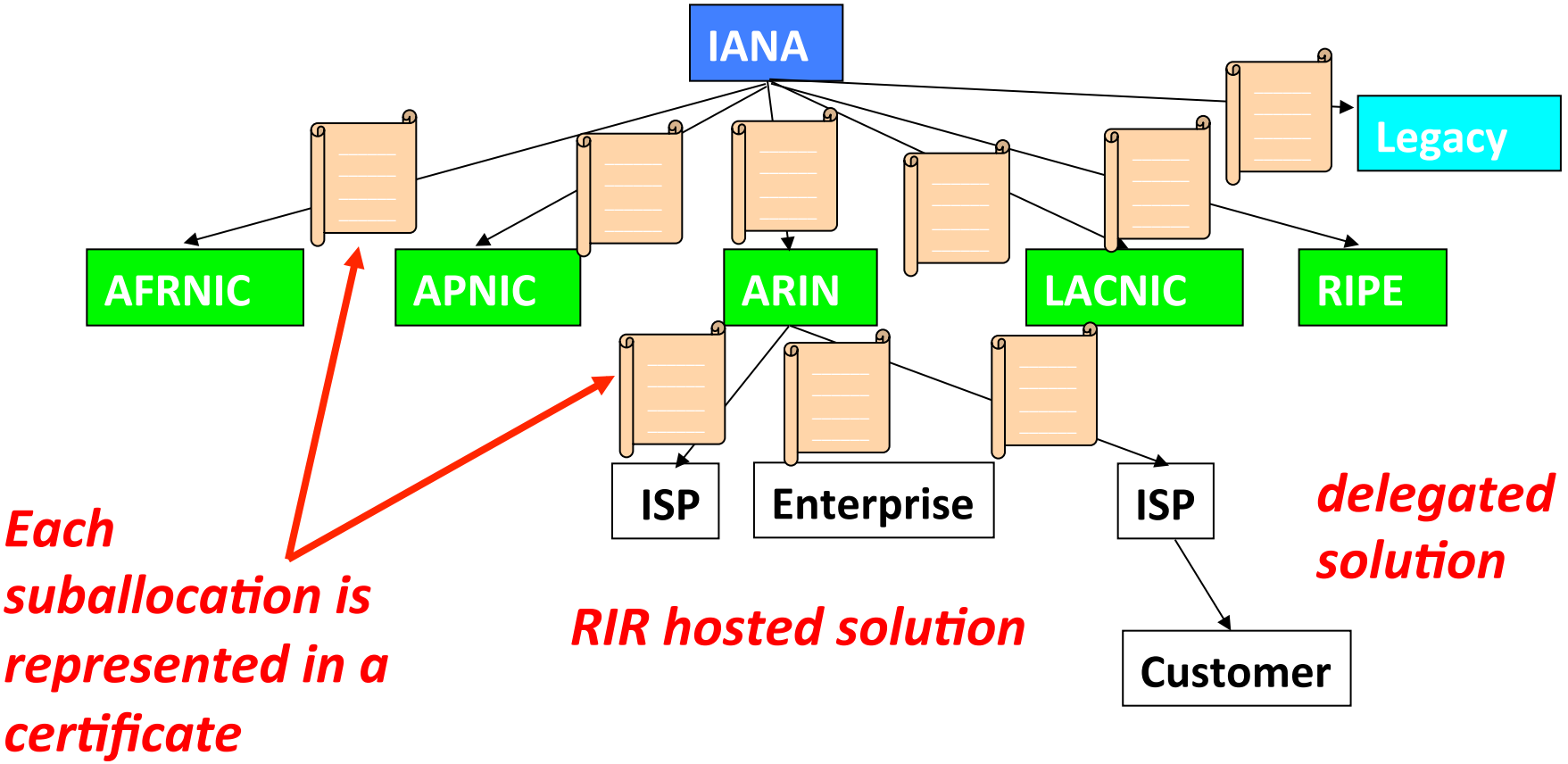
- **Origin Validation (Securing routes to ~~others'~~ addresses)**
  - Retrieve ROAs from other CA repositories
  - Validate received routes against the RPKI data
- *Think of this as checking the back of a credit card presented to you*
- *or prefix filtering*

RIR Hosted service

"Delegated" service

OOB retrieval & crypto

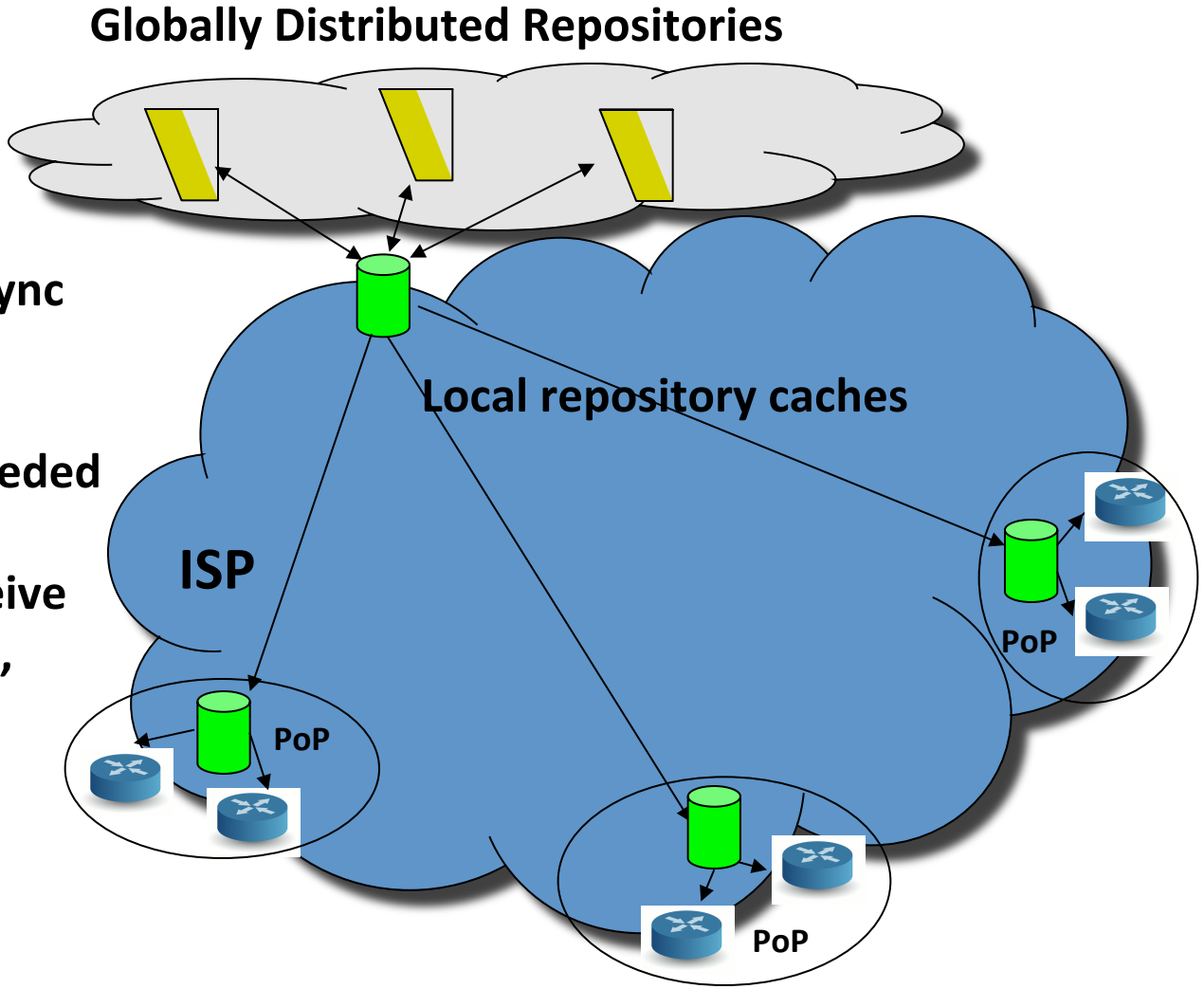
RPKI - Resource Certificates



<u>*Resource*</u> certificate, not identity certificate

RPKI Origin Validation in Single AS

- Local cache is kept in sync with global distributed repositories
- Local cache does all needed crypto
- Routers need only receive list of (authorized origin, address) pairs
- NO crypto in the routers



Track Agenda

- RPKI Introduction
  - Doug Montgomery/NIST, Sandra Murphy/PARSONS
- ARIN RPKI Services
  - Mark Kosters / ARIN – Users' guide to ARIN RPKI services.
- RPKI Implementations
  - Doug / Sandy – Quick survey of RPKI software components.
- Router Vendor Implementations
  - Keyur Patel & Arjun Sreekantiah/Cisco, John Scudder/Juniper, Greg Hankins/ Nokia
- RPKI Test, Training, Monitoring, Management, tools.
  - Matthias Wählisch/FU Berlin, Doug Montgomery, Sandy Murphy
- Deployment Experiences Panel
  - JR Mayberry/Microsoft, Tony Tauber/Comcast, Thomas King/ DE-CIX Henk Steenman/AMS-IX

Regional RPKI Services

- For certification, the one who allocated your addresses to you is the one that certifies that allocation
- **For the North American region, that is ARIN**
- RPKI services in other regions:
  - AFRINIC:
    - http://afrinic.net/en/initiatives/rpki-certification
  - APNIC:
    - http://www.apnic.net/services/services-apnic-provides/resource-certification
  - LACNIC:
    - https://rpki.lacnic.net/rpki/
  - RIPE NCC:
    - http://www.ripe.net/certification/

Track Agenda

- RPKI Introduction
  - Doug Montgomery/NIST, Sandra Murphy/PARSONS
- ARIN RPKI Services
  - Mark Kosters / ARIN – Users' guide to ARIN RPKI services.
- RPKI Implementations
  - Doug / Sandy – Quick survey of RPKI software components.
- Router Vendor Implementations
  - Keyur Patel & Arjun Sreekantiah/Cisco, John Scudder/Juniper, Greg Hankins/ Nokia
- RPKI Test, Training, Monitoring, Management, tools.
  - Matthias Wählisch/FU Berlin, Doug Montgomery, Sandy Murphy
- Deployment Experiences Panel
  - JR Mayberry/Microsoft, Tony Tauber/Comcast, Thomas King/ DE-CIX Henk Steenman/AMS-IX

RPKI Implementations

- To use RPKI data for BGP origin validation, you will want to deploy one or more "validating caches".
  - These tools collect and cache global RPKI data, perform X.509 validation on the objects,
  - … and then provides a highly summarized version to eBGP speaking routers.
  - The RPKI-to-RTR protocol enables eBGP routers to download this processed data for route filtering.
- Multiple open source validating cache implementations are available ….

RPKI Implementations

- RIPE RPKI Validator
  - https://www.ripe.net/manage-ips-and-asns/resource-management/certification/tools-and-resources
  - Validating Cache
  - Repository Fetch
    - RSYNC
    - RRDP (RPKI Repository Delta Protocol)
  - Service Interface
    - rpki-rtr protocol
  - Mgmt Interfaces
    - Web GUI, REST API, CLI (outdated)
  - Distribution
    - App / Java source
  - Support
    - RIPE NCC
- Dragon Research Labs rpki.net
  - https://rpki.net/
  - Validating Cache
  - Certificate Authority
  - Repository Fetch
    - RSYNC
    - RRDP
  - Service Interface
    - rpki-rtr protocol
  - Mgmt Interfaces
    - Web GUI, CLI
  - Distribution
    - Binary / Python source
  - Support
    - Open source; rpki@rpki.net

RPKI Implementations

- BBN Technologies RPSTIR
  - https://github.com/bgpsecurity/rpstir
  - Validating Cache
  - Repository Fetch
    - Rsync
  - Service Interface
    - rpki-rtr protocol
  - Mgmt Interfaces
    - CLI
  - Distribution
    - C source
  - Support
    - Open Source

Track Agenda

- RPKI Introduction
  - Doug Montgomery/NIST, Sandra Murphy/PARSONS
- ARIN RPKI Services
  - Mark Kosters / ARIN – Users' guide to ARIN RPKI services.
- RPKI Implementations
  - Doug / Sandy – Quick survey of RPKI software components.
- Router Vendor Implementations
  - Keyur Patel & Arjun Sreekantiah/Cisco, John Scudder/Juniper, Greg Hankins/ Nokia
- RPKI Test, Training, Monitoring, Management, tools.
  - Matthias Wählisch/FU Berlin, Doug Montgomery, Sandy Murphy
- Deployment Experiences Panel
  - JR Mayberry/Microsoft, Tony Tauber/Comcast, Thomas King/ DE-CIX Henk Steenman/AMS-IX

Router Vendor Implementations

- Origin Validation requires a router that can:
  - Interface with a RPKI validating cache to download lists of authorized origins:
    - <prefix, max_length, origin_AS>, …..
  - Match incoming BGP updates against the list of authorized origins.
  - Enforce local policies based upon on the results of these matches:
    - Valid, Invalid, Unknown
- Major router vendors support these capabilities in shipping products today!

Track Agenda

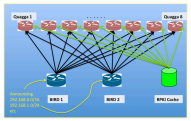
- RPKI Introduction
  - Doug Montgomery/NIST, Sandra Murphy/PARSONS
- ARIN RPKI Services
  - Mark Kosters / ARIN – Users' guide to ARIN RPKI services.
- RPKI Implementations
  - Doug / Sandy – Quick survey of RPKI software components.
- Router Vendor Implementations
  - Keyur Patel & Arjun Sreekantiah/Cisco, John Scudder/Juniper, Greg Hankins/ Nokia
- RPKI Test, Training, Monitoring, Management Tools.
  - Matthias Wählisch/FU Berlin, Doug Montgomery, Sandy Murphy
- Deployment Experiences Panel
  - JR Mayberry/Microsoft, Tony Tauber/Comcast, Thomas King/ DE-CIX Henk Steenman/AMS-IX

RPKI Test, Training, Experimentation, Monitoring, Management, etc.

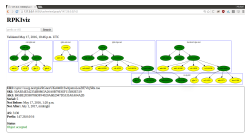
- What Resources Exists to help us:
  - Learn about RPKI provisioning and origin validation?
  - Monitor the state of RPKI deployment and my resources in particular?
  - Manage the deployment of origin validation services?
  - Experiment with implementations / software routers?

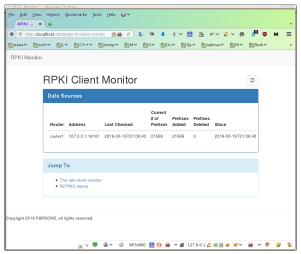
EARS Tools

- See securerouting.net
- Tools:
  - Workshop-in-a-box
    - See videos securerouting.net/workshop
  - Emulation and Operation Monitoring
  - RPKI Visualization
  - RPKI Monitor

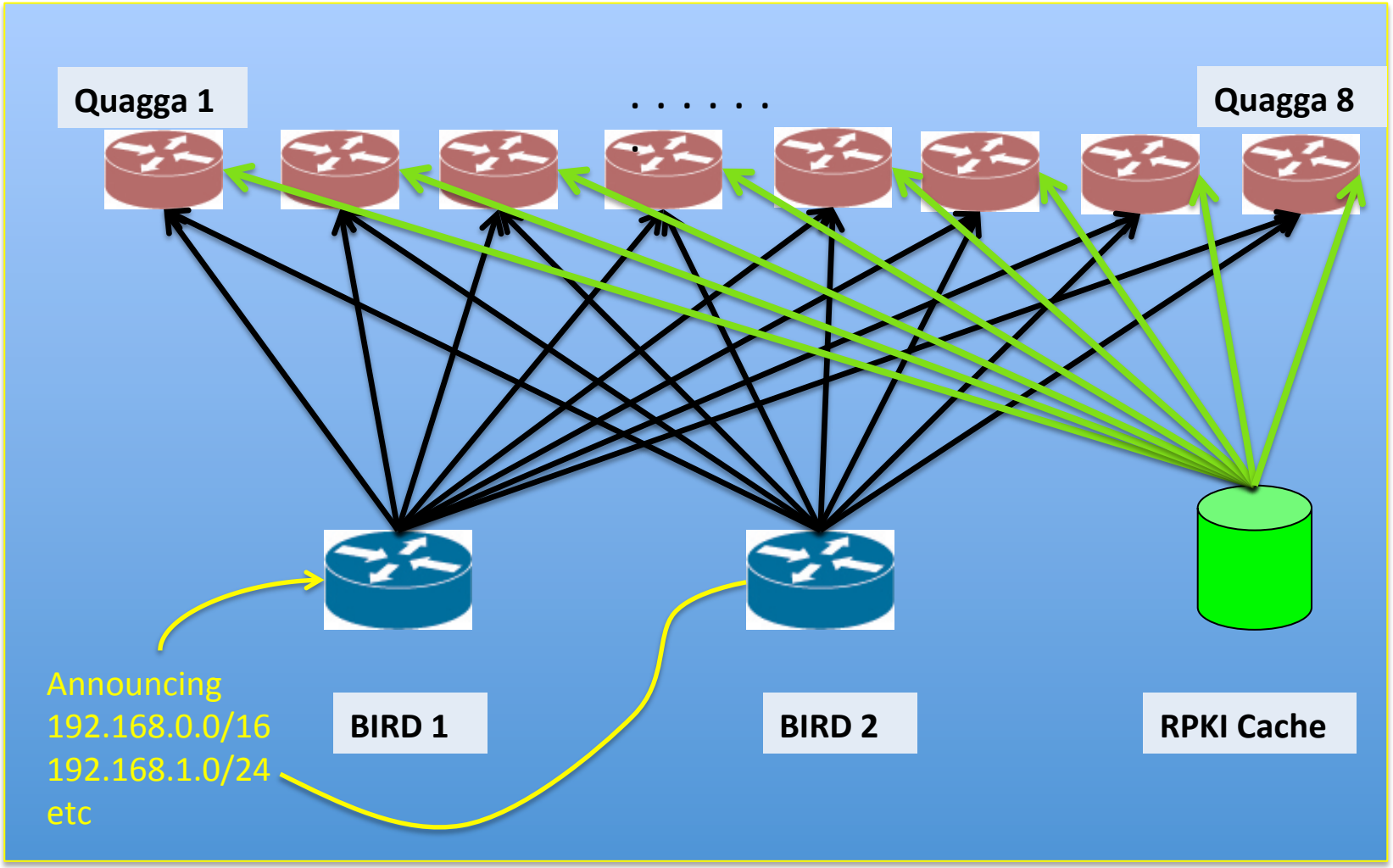








Workshop in a Box

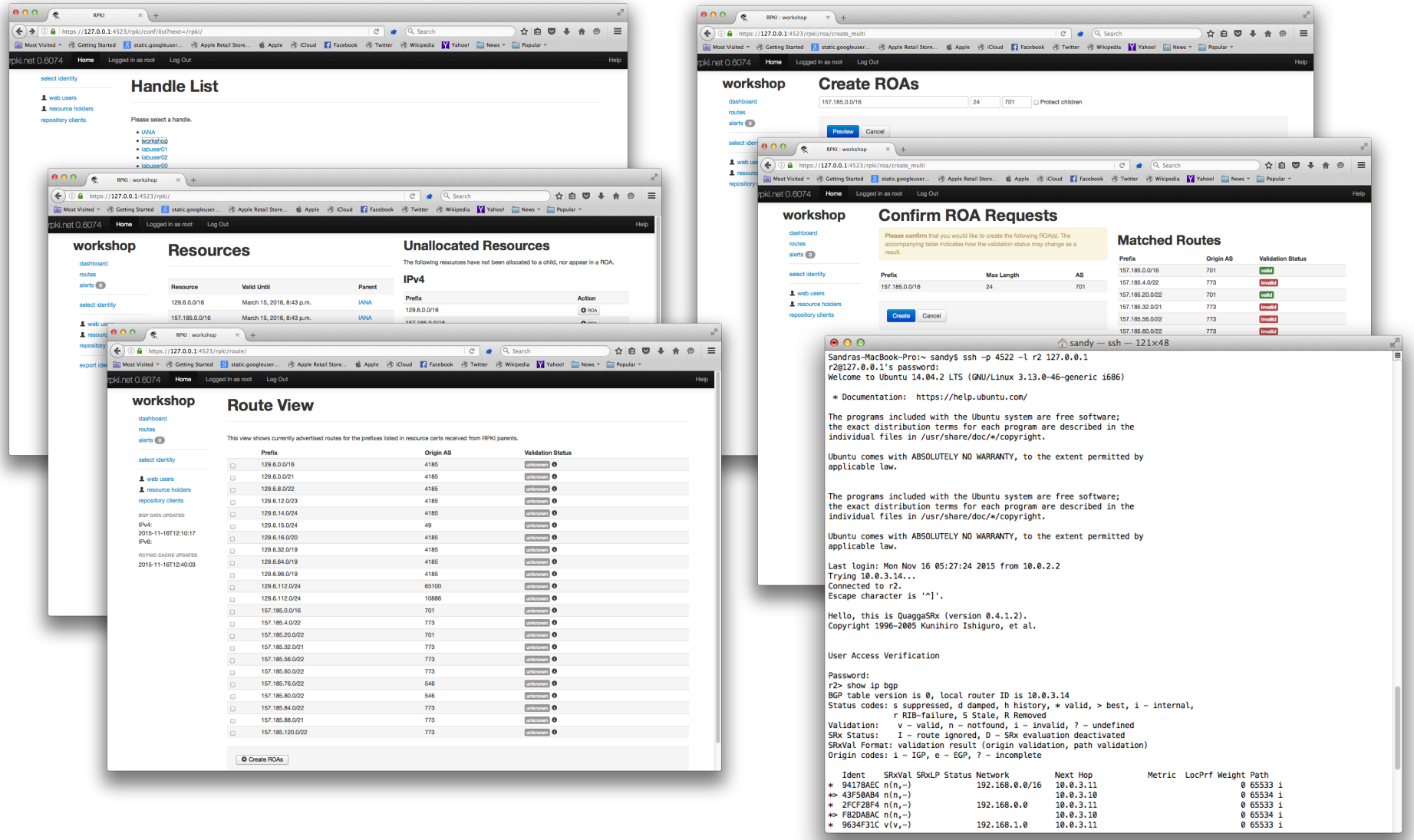


VM totally self-contained environment – no outside dependencies

Comes with local trust anchor so you can generate certs for your own prefixes

Use for experimentation, training, testing, whatever

Workshop In a Box



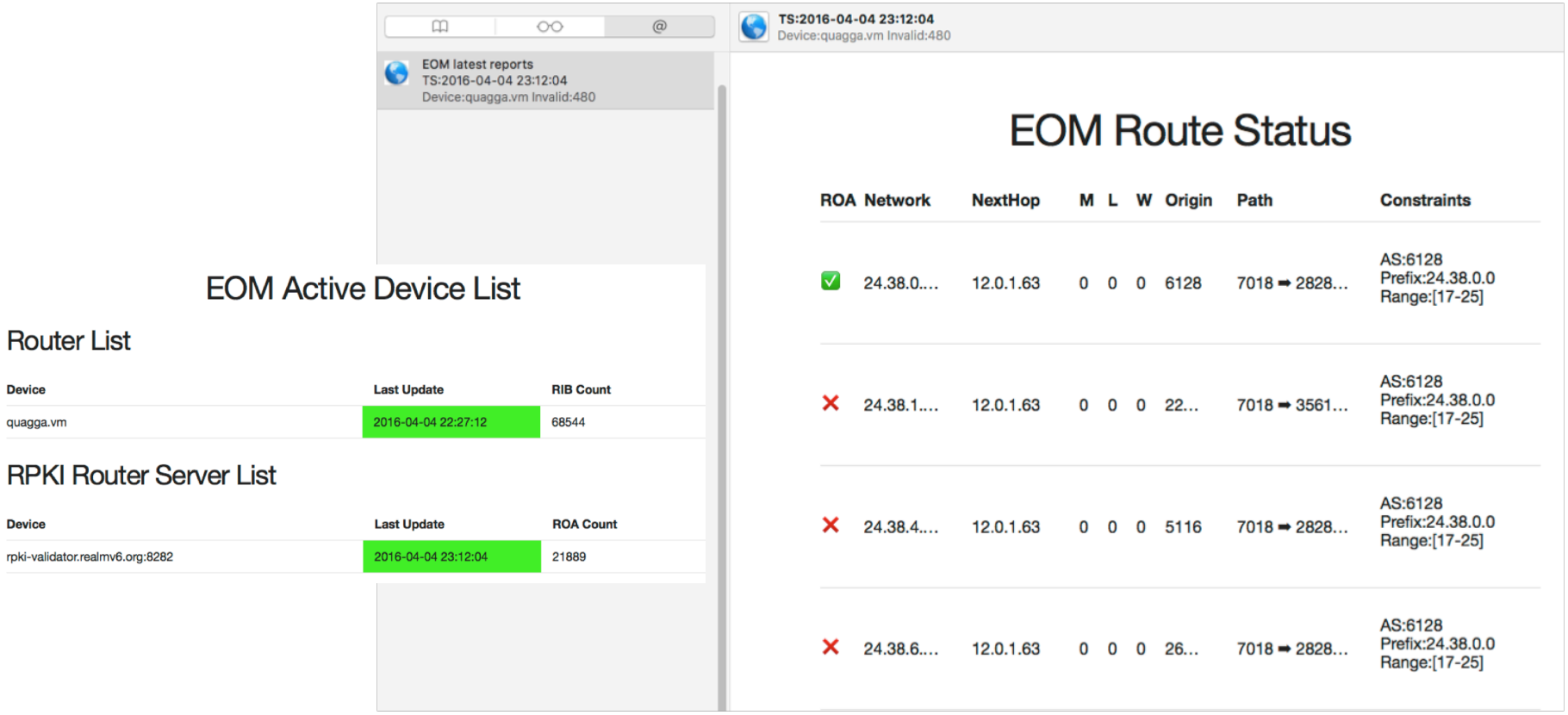
EOM (Emulation and Operation Monitoring)

Output route validation
states & why (certs)

Check local incoming routes against RPKI data
Intended use:

- What RPKI would say about your current feeds - without deploying RPKI
- Monitor routing table RPKI state during deployment

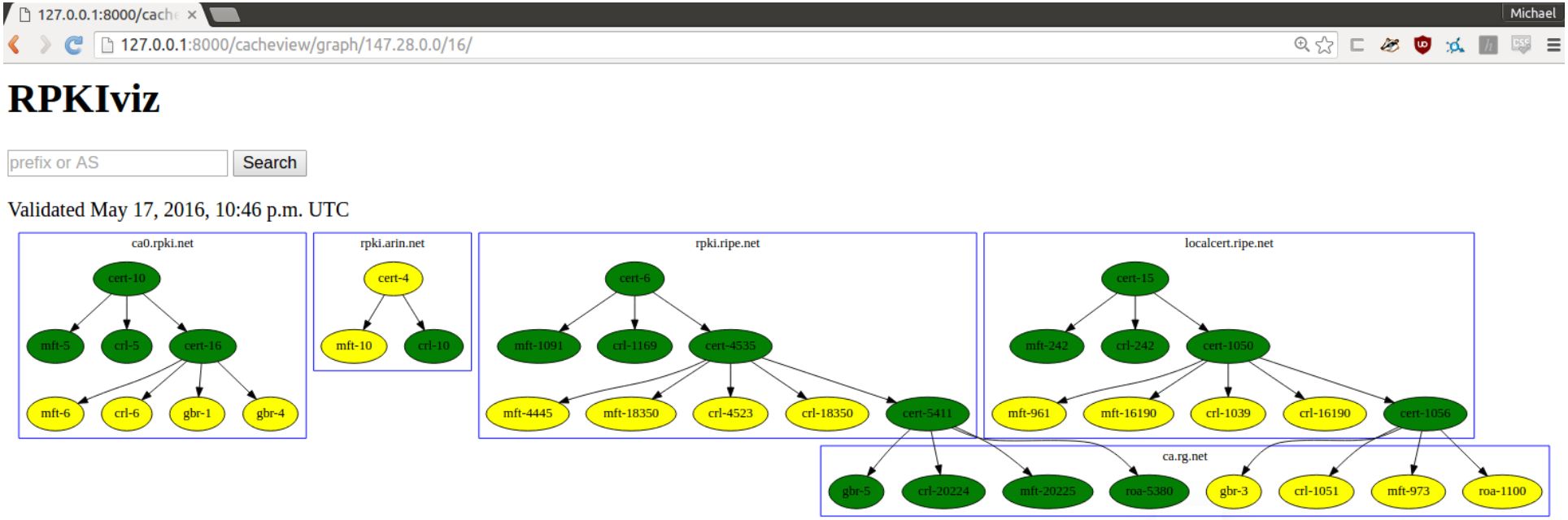
EOM (Emulation and Operation Monitoring) - GUI



EOM (Emulation and Operation Monitoring) - CLI

```
Router: 172.16.0.6
      Network          Next Hop Metric     LocPrf     Weight    Path
V : * 10.1.1.0/24      172.16.0.5       0      0      0      65005 65004   i
      65004:10.1.1.0/[24-24]
V : *>      10.1.1.0/24      172.16.0.4       0      0      0      65004      i
      65004:10.1.1.0/[24-24]
I : *>10.1.1.0/25      172.16.0.5       0      0      0      65005 65004 65004 65004 65004  i
      65004:10.1.1.0/[24-24]
I : *>10.1.1.128/25 172.16.0.5       0      0      0      65005 65004 65004 65004 65004  i
      65004:10.1.1.0/[24-24]
```

Monitor: RPKI Visualization

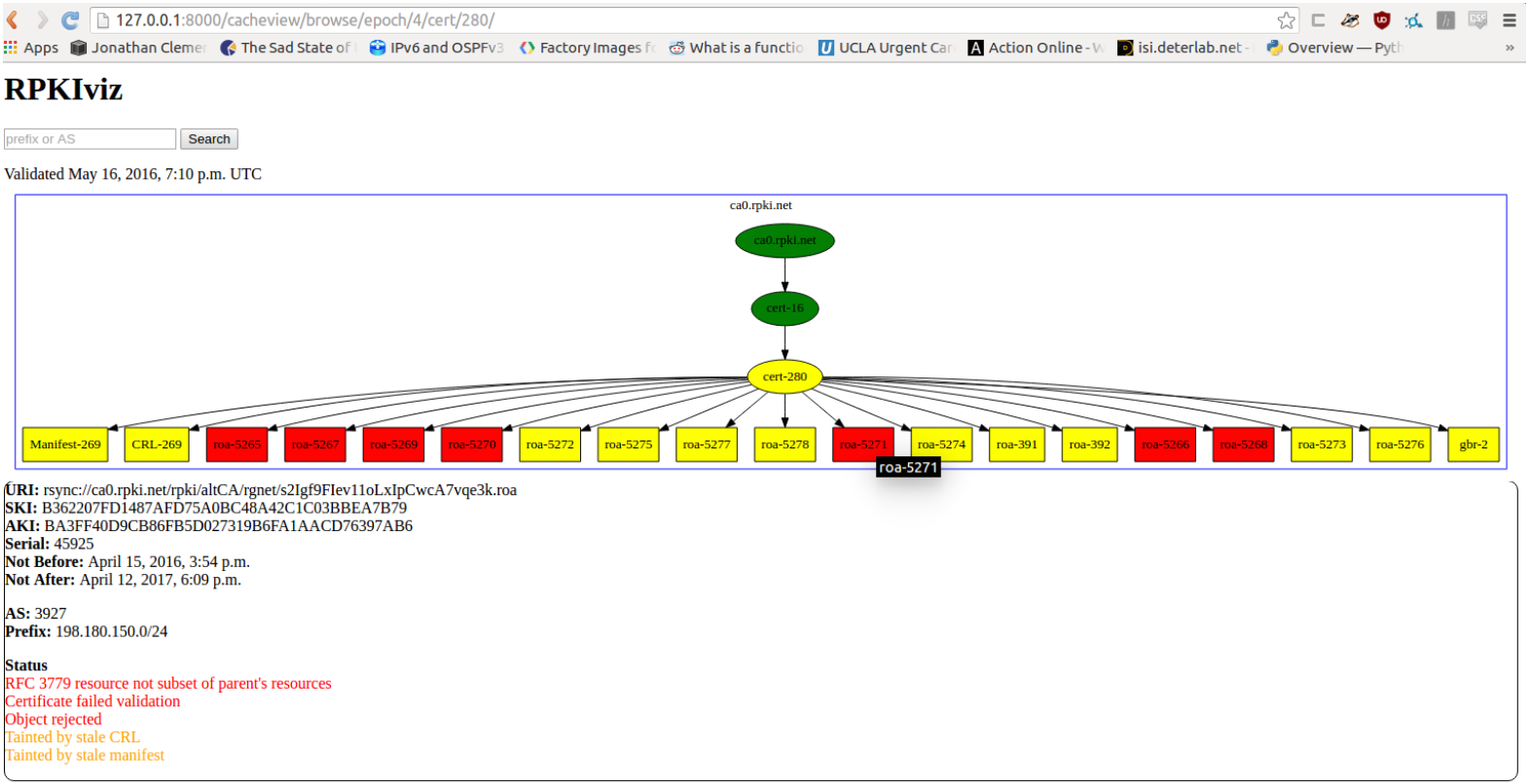


URI: rsync://ca.rg.net/rpki/RGnet/UKs040I1SwhjomoLeeZfEVhj5Rk.roa
SKI: 50AB34E342354B0863A26A0B79E65F115863E519
AKI: B45BE20598786DFF4020A6B2947D5333A0A04A2B
Serial: 5
Not Before: May 17, 2016, 1:20 p.m.
Not After: July 1, 2017, midnight

AS: 3130
Prefix: 147.28.0.0/16

Status
Object accepted

Monitor: RPKI Visualization



Errors

Monitor: RPKI Visualization

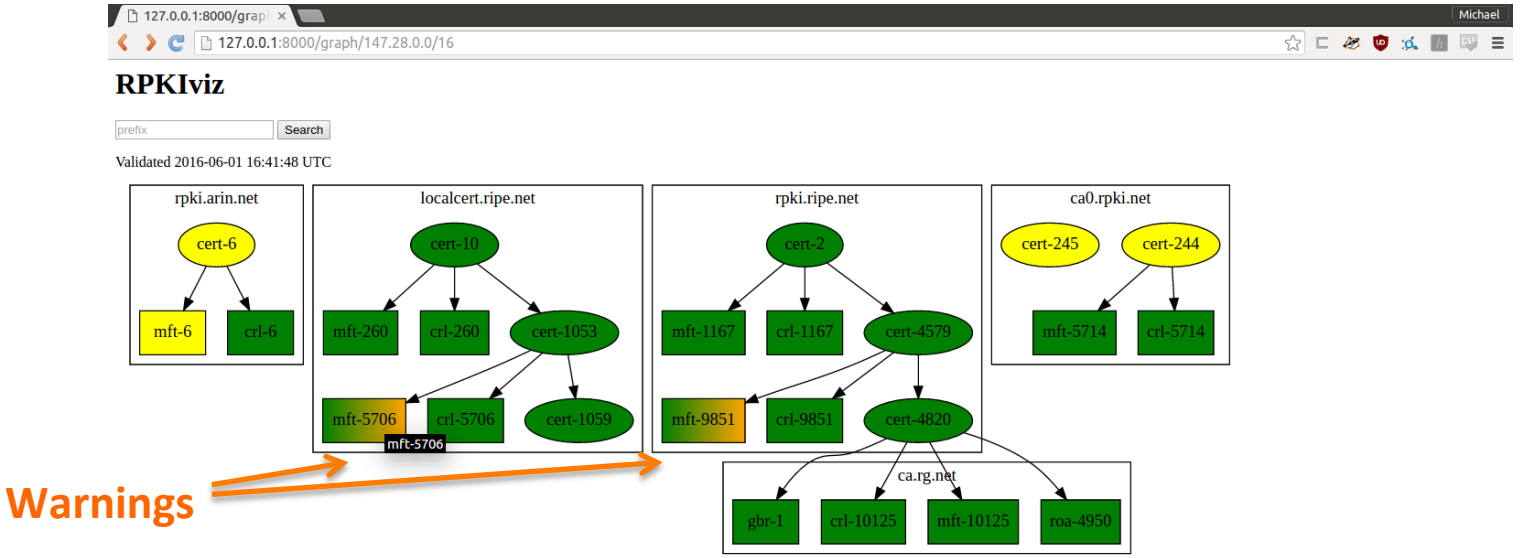
192.169.0.0/23 History

2016-05-10 23:59:38 to **2016-05-11 19:21:06**

When	Status	ROAs	Certs
2016-05-10 23:59:38	covered	AS3970	BA3FF... 621A0... A6B69...
2016-05-11 01:15:54	covered	AS3970	BA3FF... 621A0... A6B69...
2016-05-11 04:43:39	covered	AS3970	BA3FF... 621A0... A6B69...
2016-05-11 13:54:45	covered	AS3970	BA3FF... 621A0... A6B69...
2016-05-11 14:21:03	covered	AS3970	BA3FF... 621A0... A6B69...
2016-05-11 15:21:24	covered	AS3970	BA3FF... 621A0... A6B69...
2016-05-11 16:21:21	covered	AS3970	BA3FF... 621A0... A6B69...
2016-05-11 17:44:13	covered	AS3970	BA3FF... 13D4F... 621A0... A6B69...
2016-05-11 18:22:29	covered	AS3970	BA3FF... 13D4F... 621A0... A6B69...
2016-05-11 18:30:42	covered	AS3970	BA3FF... 13D4F... 621A0... A6B69...
2016-05-11 19:21:06	covered	AS3970	BA3FF... 13D4F... 621A0... A6B69...

History

Monitor: RPKI Visualization



URI: rsync://localcert.ripe.net/repository/ARIN/z-P1LDkk4VCC5gayNA17GkCisdM.mft

Issuer: /commonName=cfe3f52c3924e15082e606b2340d7b1a40a2b1d3
Subject: /commonName=adb4a3910cee6bc15d9e1c8df20e3b16aac8f6cd
AKI: CFE3F52C3924E15082E606B2340D7B1A40A2B1D3
SKI: ADB4A3910CEE6BC15D9E1C8DF20E3B16AAC8F6CD
Serial: 312462643
Not Before: 2016-06-01 10:35:53
Not After: 2016-06-08 10:40:53

thisUpdate: 2016-06-01 10:40:53
nextUpdate: 2016-06-02 10:40:53
manifestNumber: 856
File Hash Algorithm: 2.16.840.1.101.3.4.2.1

Status
Object accepted

Filename	Hash
BmcfKPv7cTiXTQAfOFyT0r6vEnI.cer	4585b1a9a7898c3b5da5f1e0beb88c8cf972cf877bf4d3500fc6c5830d97e68f
OMsJ1MFs0bKupi9QEv1GVQZd_Cg.cer	d21d7b553f1ad081be25a2b3a93e74a3b09214cb573cdab6c3e0ab341bf9a821
Q0mhaoNsC9KSA4DrjpsRzjhTLvA.cer	578724f6369a9e5c70b2138314d18de6cd5080dd9826e7c711a9e69f2c44e73c
S5P_i37gvDVh9qBi80oPOXkFhp0.cer	45d857ce09e8eb55b09da53435b705ae80973f8d517cfd8630cd063211a67c43
gLgYkg0P-Q_WVKHqel_DnB7cuSc.cer	4c3eb0142e9e92029f57f4649bd790547473a28c317c265bf17806eebf762ac0
ggRF6wI0nMPjABu3TqJC2SNv2fA.cer	6dca646816d4ad3260996bca9e990291b71a8692c534df2a5330448232b1ef15
z-P1LDkk4VCC5gayNA17GkCisdM.crl	88e9e18bf1a50646b5d1ced63161fc8cde6ccc6d88d2a985f83a97d33de13565

Track Agenda

- RPKI Introduction
  - Doug Montgomery/NIST, Sandra Murphy/PARSONS
- ARIN RPKI Services
  - Mark Kosters / ARIN – Users' guide to ARIN RPKI services.
- RPKI Implementations
  - Doug / Sandy – Quick survey of RPKI software components.
- Router Vendor Implementations
  - Keyur Patel & Arjun Sreekantiah/Cisco, John Scudder/Juniper, Greg Hankins/ Nokia
- RPKI Test, Training, Monitoring, Management, tools.
  - Matthias Wählisch/FU Berlin, Doug Montgomery, Sandy Murphy
- Deployment Experiences Panel
  - JR Mayberry/Microsoft, Tony Tauber/Comcast, Thomas King/ DE-CIX Henk Steenman/AMS-IX