
RPKI deployment at AFRINIC Status Update

Alain P. AINA
RPKI Project Manager



What is Resource Certification ?

Resource Certification is a security framework for verifying the association between resource holders and their Internet resources.

Add a verifiable form of a holder's current “right-of-use” over Internet resources in the resources management system

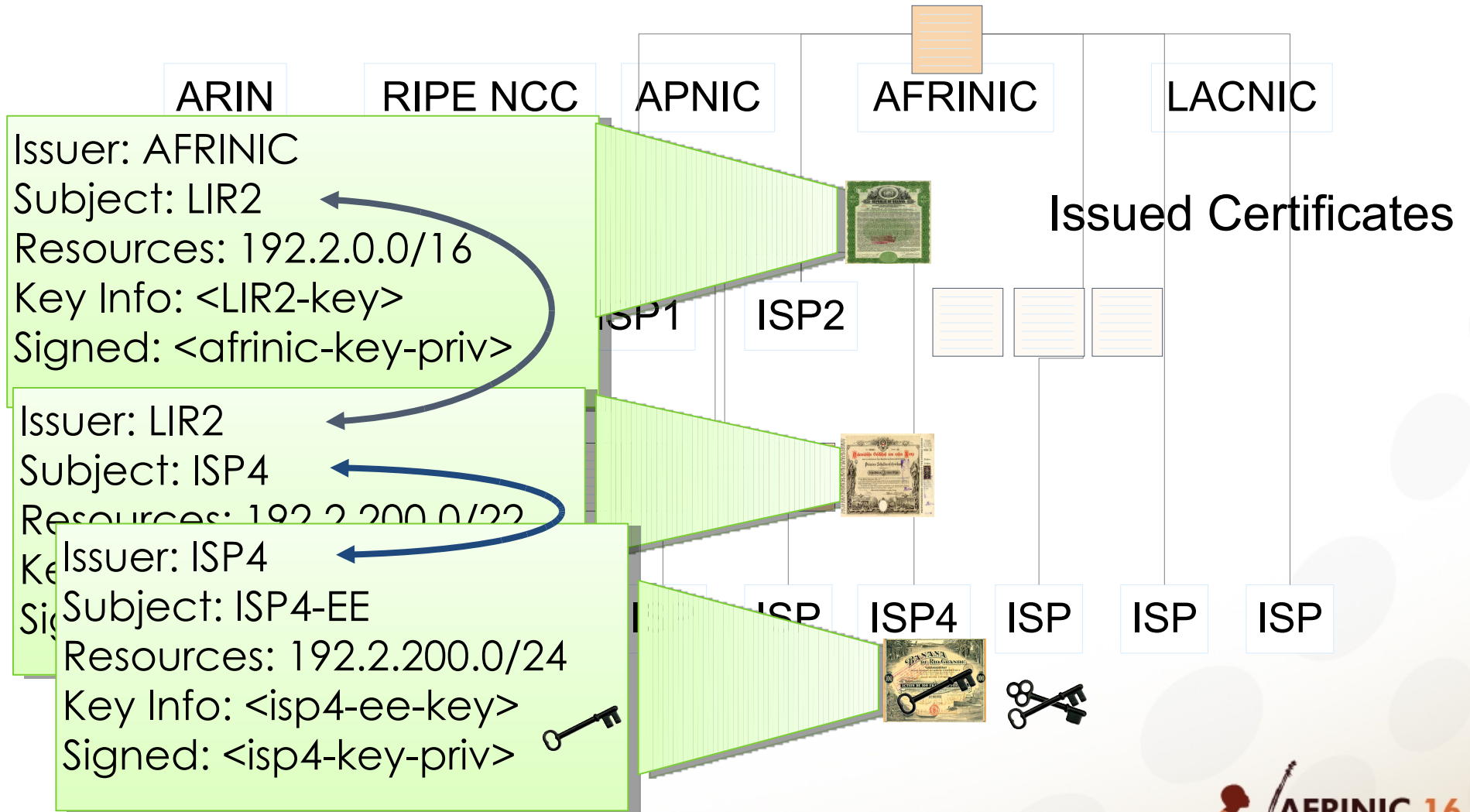
Resource Public Key Infrastructure(RPKI) is a PKI based on the Internet resources management hierarchy and under which X509 certificates with RFC 3779 extensions and other signed objects are published and bound together in an verifiable way.

Motivations for RPKI

- Facilitate better routes filtering
- Prepare for a secure routing
- Solve the chicken-and-egg problem
- Provide trusted data
Better than the current Whois and IRR data
- Post IPv4 exhaustion data accuracy
Resource transfers

Resource Certificates

Resource
Allocation
Hierarchy



Services for the RPKI

Intended AFRINIC services for LIRs

- **Certify LIR resources using the AFRINIC's RPKIE**
 - **Provide hosted RPKI services for LIRs:**
 - *A full managed RPKIE for LIR*
 - *Run the LIR's RPKIE et give real control to LIRs*
 - **Deploy the UP-Down protocol to talk to LIR willing to run their own RPKIE**
 - **Provide the necessary public repository**
 - **Access to these services:**
 - *Through the normal channels (MyAFRINIC)*
 - *With strong authentication*
- X509 Auth with BPKI certs*

RPKI initial Roadmap

4 Phases by the NRO

- **Phase 1: Pilot**
 - Operational since 15/6/2010
- **Phase 2: Initial Production**
 - 01/01/2011
- **Phase 3: Global Consistency**
 - 01/09/20??
- **Phase 4: Single Trust Anchor**
 - 01/01/20??

AFRINIC's RPKI System

- Based on APNIC code
- Integrated into myAFRINIC
- Current TA cover
 - IPv4: (41-196-197)/8
 - IPv6: 2001:4200::/23 ; 2C00:0000::/12
 - ASNs: all listed “assigned by AFRINIC” at <http://www.iana.org/assignments/as-numbers/as-numbers.xml>
- Open for the community since 01/01/2011
 - <http://www.afrinic.net/membership/certification.htm>

RIRs Deployment Status

- Each RIR has completed Phase 1 and 2
- Implemented the TAL
 - <http://tools.ietf.org/wg/sidr/draft-ietf-sidr-ta/>
- Working on Phase 3
- Following the single TA discussions with ICANN

Firefox File Edit View History Bookmarks Tools Window Help
Index of /
afrinic.net https://rpki.afrinic.net/
Most Visited - Getting Started Latest Headlines Features/DNSSEC IETF Journal-IETF-K... Whois v3 object tem... The Dell Online Stor... draft-change 32bit ... RIPE Da
African Network Informatio... Apple - Start African Network Informatio... African Network Informatio... Index of /

Index of /

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 member_repository/	16-Nov-2010 15:09	-	
 repository/	19-Jul-2010 12:59	-	

Apache/2.2.3 (CentOS) Server at rpki.afrinic.net Port 443

Also available through rsync
rsync://rpki.afrinic.net

SIDR WG status

- First RFCs published in 02/2012
 - RFC 6480 to RFC 6494
 - RPKI design and implementation standards
- draft-ietf-sidr-rpki-rtr approved by IESG and in RFC editor queue
- BGPSEC in the pipe

<http://tools.ietf.org/wg/sidr/>

Statistics: RPKI Engines –17 members

- African Network Information Center - (AfriNIC Ltd)
- Access Communications Ltd
- Wireless Business Solutions (Proprietary) Limited t.a iBurst
- Beltone Financial
- Sentech Ltd
- University of Lagos
- Internet Solutions
- Clickatell PTY(LTD)
- Satcom Networks Africa

Statistics: RPKI Engines(Cont.d)

- African Network Operators' Group (AFNOG)
- ISPA SA
- ETISALAT MISR
- Compute Corporate Technology Solutions
- TATA Communications
- MWEB CONNECT (PROPRIETARY) LIMITED
- Libyan Telecom and Technology

Statistics: Signed objects

RPKI Validator - Configured Trust Anchors

http://127.0.0.1:8080/trust-anchors

Router Allo...sco Systems Cisco IOS Se...sco Systems network aut...rche Google http://www....mniPCX.pdf End-of-Sale...sco Systems

RPKI Validator - Configured Trus...

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

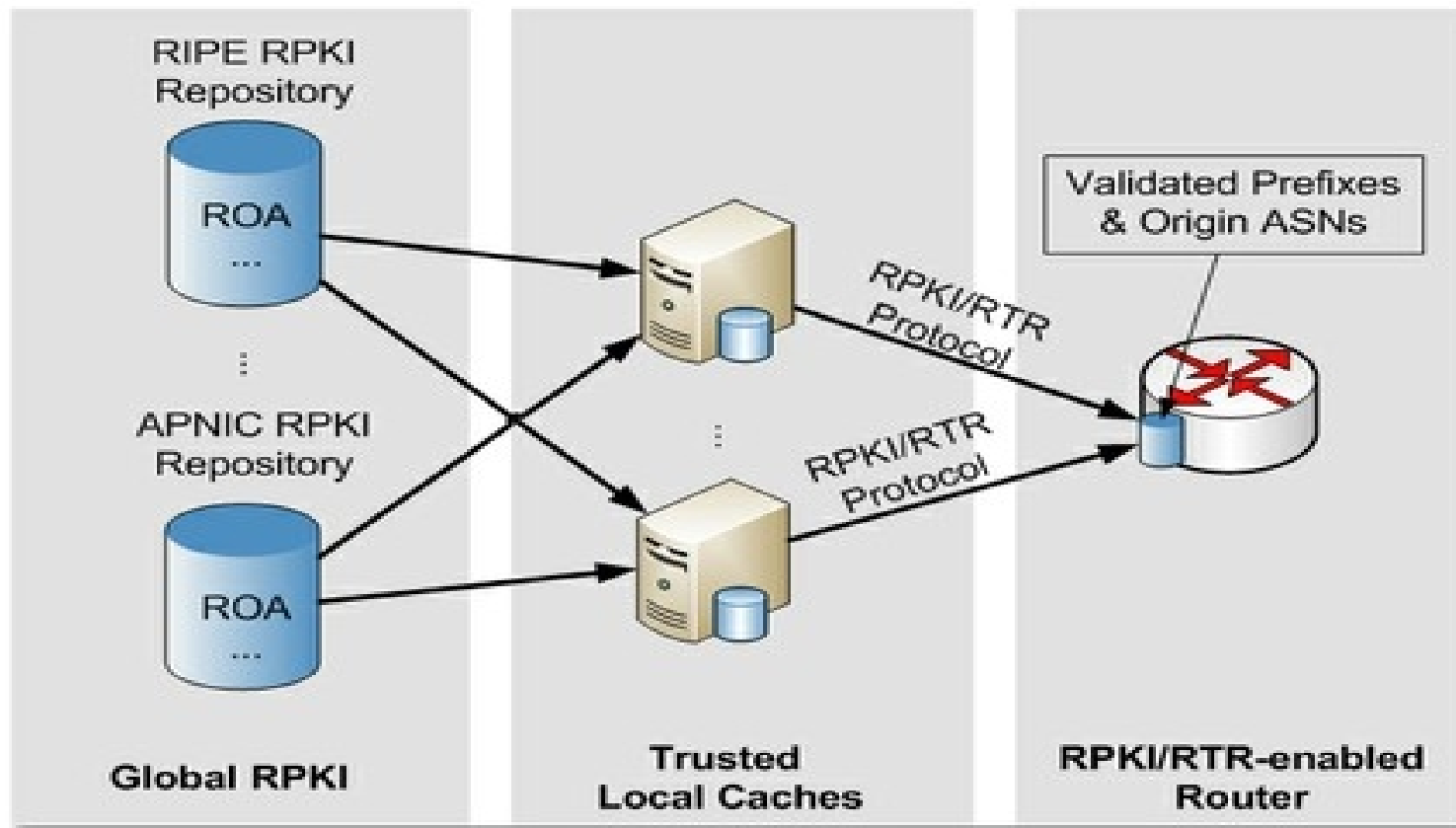
New version 2.3 available [here](#).

Configured Trust Anchors

Enabled	Trust anchor	Processed Items	Expires in	Last updated	Next update in	Update all
<input checked="" type="checkbox"/>	APNIC RPKI Root	1374 0 0	4 years and 1 month	15 minutes ago	3 hours	Update
<input checked="" type="checkbox"/>	ARIN Test Lab	88 88 0	1 year and 1 month	16 minutes ago	3 hours	Update
<input checked="" type="checkbox"/>	AfriNIC RPKI Root	77 0 1	4 years and 6 months	16 minutes ago	3 hours	Update
<input checked="" type="checkbox"/>	LACNIC RPKI Root	233 0 0	9 months and 3 weeks	16 minutes ago	3 hours	Update
<input checked="" type="checkbox"/>	RIPE NCC RPKI Root	3654 0 0	4 years and 11 months	15 minutes ago	3 hours	Update

Feedback

RPKI and BGP origin Validation



<http://tools.ietf.org/wg/sidr/draft-ietf-sidr-rpki-rtr/>

RPKI and BGP origin Validation

```
rpki-rtr>sh bgp ipv4 unicast 196.216.2.0
```

BGP routing table entry for 196.216.2.0/23, version 404049

Paths: (2 available, best #1, table default)

Not advertised to any peer

Refresh Epoch 1

12654 3741 33764

193.0.4.1 from 193.0.4.28 (193.0.4.28)

Origin IGP, localpref 110, valid, external, best
path 5BFFCC28 **RPKI State valid**

Refresh Epoch 1

12654 3741 33764, (received-only)

193.0.4.1 from 193.0.4.28 (193.0.4.28)

Origin IGP, localpref 100, valid, external
path 5BFFCBE4 **RPKI State valid**

196.216.2.0/23 covered by a ROA

RPKI and BGP origin Validation

```
rpki-rtr>sh bgp ipv4 unicast 196.200.57.0
```

BGP routing table entry for 196.200.48.0/20, version 113775

Paths: (2 available, best #1, table default)

Not advertised to any peer

Refresh Epoch 1

12654 3549 6453 8346 30985 36864

193.0.4.1 from 193.0.4.28 (193.0.4.28)

Origin IGP, localpref 100, valid, external, best

Community: 232589365 232618104

path 2379CEC4 **RPKI State not found**

Refresh Epoch 1

12654 3549 6453 8346 30985 36864, (received-only)

193.0.4.1 from 193.0.4.28 (193.0.4.28)

Origin IGP, localpref 100, valid, external

Community: 232589365 232618104

path 2379CE80 **RPKI State not found**

196.200.48.0/20 not covered by a ROA

Questions ?

