RPKI deployment at AfriNIC Status Update

AfriNIC-14
Dar El Salaam, 09/06/2011

Alain P. AINA
RPKI Project Manager/Spokesman
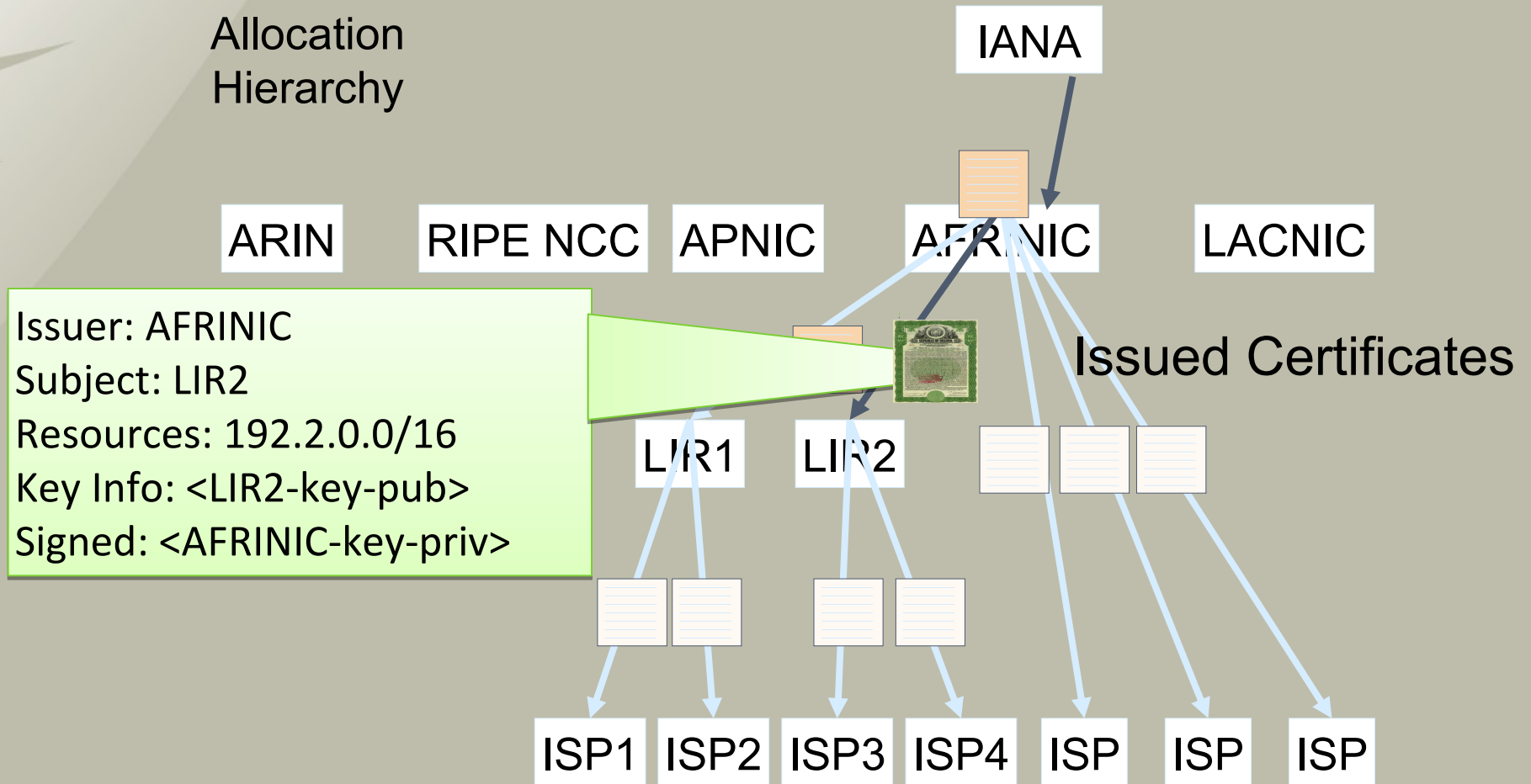
Amreesh Phokeer
Project member/Deputy Speaker

AfriNIC

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
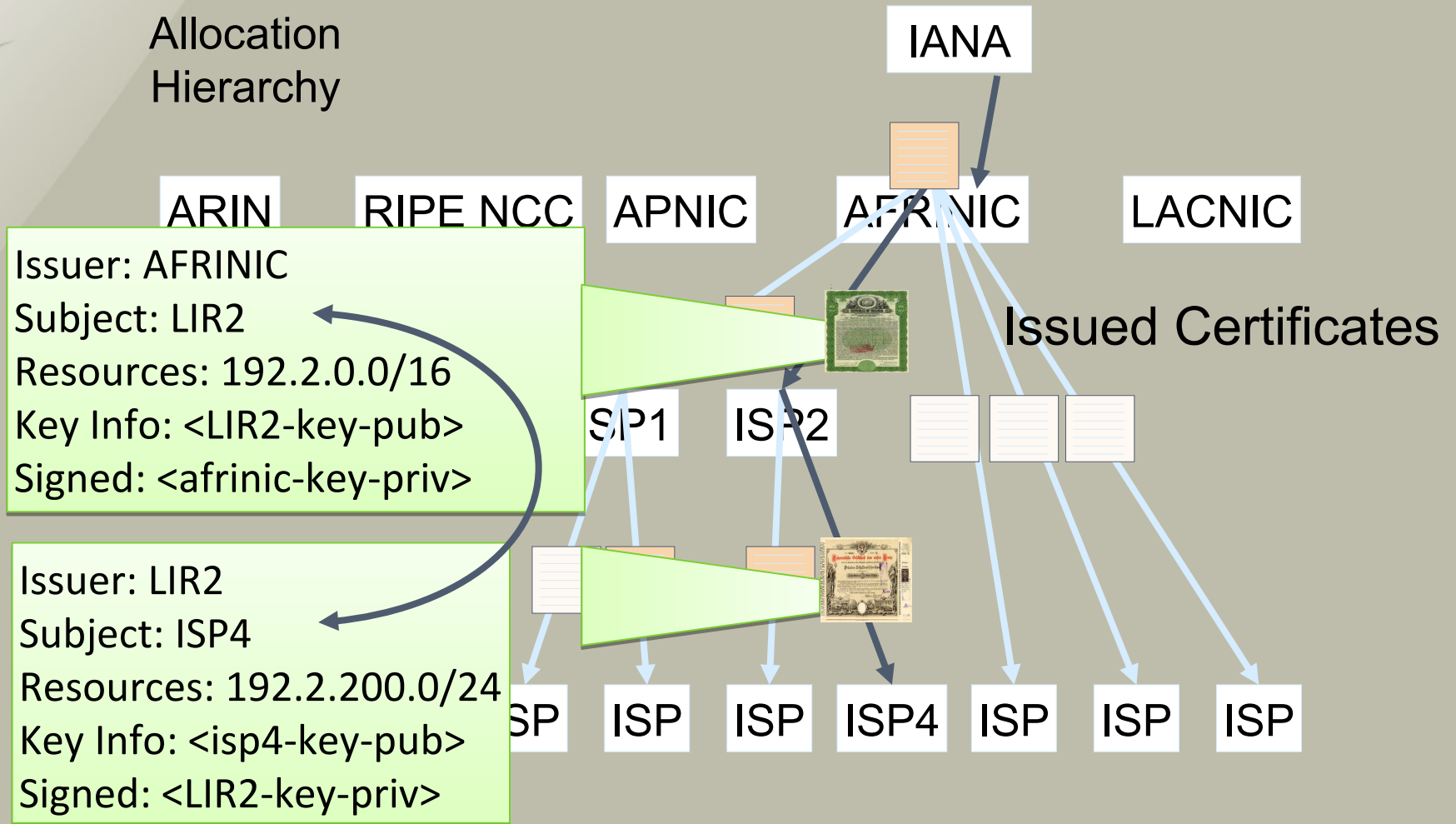
➢ **Post IPv4 exhaustion data accuracy**
   Resource transfers

Resource Certificates

Resource
Allocation
Hierarchy

IANA

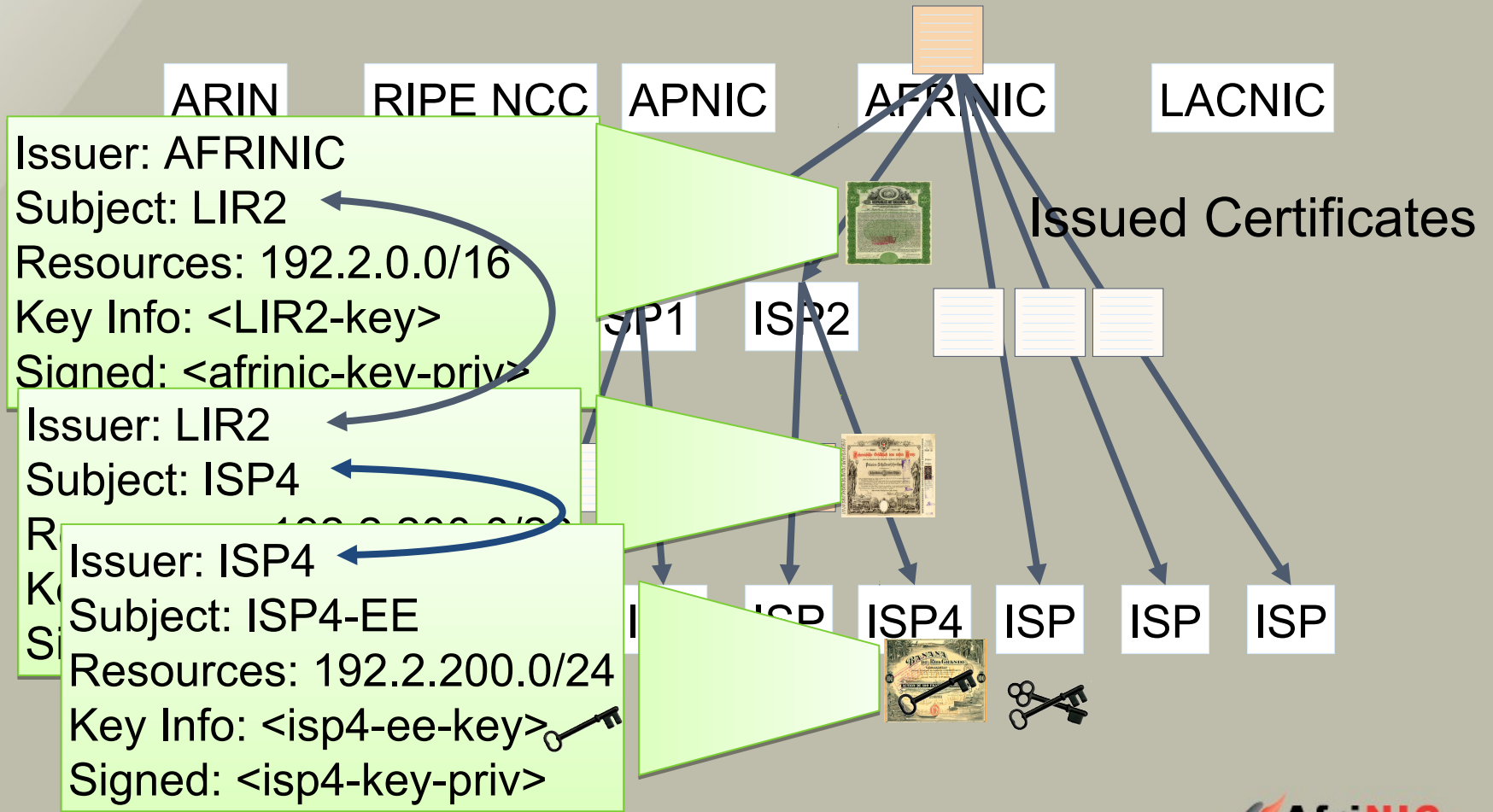ARIN   RIPE NCC   APNIC   AFRINIC   LACNIC

Issued Certificates

Issuer: AFRINIC
Subject: LIR2
Resources: 192.2.0.0/16
Key Info: <LIR2-key-pub>
Signed: <AFRINIC-key-priv>

LIR1   LIR2

ISP1   ISP2   ISP3   ISP4   ISP   ISP   ISP

AfriNIC

Resource Certificates

Resource
Allocation
Hierarchy

IANA

ARIN RIPE NCC APNIC AFRINIC LACNIC

Issued Certificates

Issuer: AFRINIC
Subject: LIR2
Resources: 192.2.0.0/16
Key Info: <LIR2-key-pub>
Signed: <afrinic-key-priv>

ISP1 ISP2

Issuer: LIR2
Subject: ISP4
Resources: 192.2.200.0/24
Key Info: <isp4-key-pub>
Signed: <LIR2-key-priv>

SP ISP ISP ISP4 ISP ISP ISP

AfriNIC

Resource Certificates

Resource Allocation Hierarchy

ARIN   RIPE NCC   APNIC   AFRINIC   LACNIC

Issued Certificates

Issuer: AFRINIC
Subject: LIR2
Resources: 192.2.0.0/16
Key Info: <LIR2-key>
Signed: <afrinic-key-priv>

Issuer: LIR2
Subject: ISP4

Issuer: ISP4
Subject: ISP4-EE
Resources: 192.2.200.0/24
Key Info: <isp4-ee-key>
Signed: <isp4-key-priv>

ISP1   ISP2

ISP4   ISP   ISP   ISP

AfriNIC

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

AfriNIC

RPKI Roadmap to Production – 4 Phases by the NRO

- **Phase 1: Pilot**
  - Operational since 15/6/2010

- **Phase 2: Initial Production**
  - 01/01/2011

- **Phase 3: Global Consistency**
  - 01/09/2011

- **Phase 4: Single Trust Anchor**
  - 01/01/2012

AfriNIC

Phase 1: Pilot

- Independent deployment
- Not necessarily consistent
  - May overclaim resources (e.g. 0/0)
- Standard
  - Resource Certificates
- Transfers are handled manually

AfriNIC

Phase 2: Initial Production

- 5 independent Trust Anchors
  - One per RIR
  - Split
    - Extended Trust Anchor (ETA)
    - Resource Trust Anchor (RTA)
- RTA reflects allocated resources
  - Minimal overclaiming
- Standard
  - Resource Certificates
  - Repositories
  - ETA/RTA
  - CP & consistent CPS's
- Inter-RIR transfers handled manually

AfriNIC

Phase 3: Global Consistency

- 5 independent ETAs
- RTAs are congruent with the IANA registry
  - No overclaiming, majority RIR for the ERX space
  - Visible consistency
- Standard
  - Resource Certificates
  - Repositories
  - ETA
  - Up-Down protocol
  - CP & consistent CPS's
- Inter-RIR transfers can be automated

AfriNIC

Phase 4: Single TA

- One Single TA
  - May be a natural 0/0
- Standard
  - Resource Certificates
  - Repositories
  - Up-Down protocol
  - CP & consistent CPS's
- Changes to the global registry and transfers can be automated

AfriNIC

RIR 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

AfriNIC

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
  - http://www.afrinic.net/membership/certification.htm

AfriNIC

African Network Information Center : Resources – Manage Your RPKI Resources

afrinic.net   https://beta.afrinic.net/resources/rpki/   Google

| isited ▾ | Getting Started | Latest Headlines 🔊 | Features/DNSSEC – … | IETF Journal–IETF–K… | Whois v3 object tem… | The Dell Online Stor… | draft–change 32bit … | RIPE Databas |

frican Network Information C… ⊗ | 🍎 | Apple – Start ⊗ | 📄 African Network Information C… ⊗ | +

AfriN

| Home | Control Panel | My Account | Billing | Resources | Help & Support |

AS Numbers   IPv4 Resources   IPv6 Resources   Reverse Delegation   Resource Certification   [Sign-Out]

a Alain Patrick @ African Network Information Center - (AfriNIC Ltd)

are here: Home > Resources > Resource Certification > Manage Your RPKI Resources

Quick Links -- ▾   Jump

Whois

Advanced Options

Calendar

November ▾   2010 ▾

Mon	Tue	Wed	Thu	Fri	Sat
1	2	3	4	5	6
8	9	10	11	12	13
15	16	17	18	19	20
22	23	24	25	26	27
29	30				

Manage Your RPKI Resources

You can manage your RPKI resources from this page

RPKI Operations

View certificates

View ROAs

Issue ROA

View AAOs

Issue AAO

Refresh engine

5.   Add **Control** to the two shortcuts above to place the screen shot on the clipboard instead of

Photoshop Elements 9

afrinic.net https://beta.afrinic.net/resources/rpki/rescert

ormation C… ⊗   Apple – Start   ⊗   African Network Information C… ⊗   +

Certificate Details

Field	Value
Version	3
Serial Number	7F:6B
Issuer	/CN=7295DF/SN=B3C25163027150E6FEAD26DF375260E4F8B0AABA
Subject	/CN=Ef68eF/SN=530FDEA82EA2C76DC1D3F3CA7A3C9945FA67B214
Not Valid Before	Nov 17 2010 0:00:05 GMT
Not Valid After	Dec 31 2010 0:00:00 GMT
Subject Key Identifier	53:0F:DE:A8:2E:A2:C7:6D:C1:D3:F3:CA:7A:3C:99:45:FA:67:B2:14
Authority Key Identifier	B3:C2:51:63:02:71:50:E6:FE:AD:26:DF:37:52:60:E4:F8:B0:AA:BA
Authority Information Access	caIssuers - rsync://rpki.afrinic.net/repository/CAFFF7A889C011DF8EDDC8A9F81ED8FE/s8JRYwJxUOb-rSbfN1Jg5Piwqro.cer
Subject Information Access	caRepository - rsync://rpki.afrinic.net/member_repository/F4D17C32914011DFA116BB5E4DC4681B/ rpkiManifest - rsync://rpki.afrinic.net/member_repository/F4D17C32914011DFA116BB5E4DC4681B/Uw_eqC6ix23B0_PKejyZRfpnshQ.mft
IPv4	41.223.236.0/22, 41.223.252.0/22, 196.1.0.0/24, 196.1.15.0/24, 196.2.3.0/24, 196.6.0.0/24, 196.216.2.0/23, 196.216.168.0/23, 196.216.254.0/24, 196.223.150.0/23, 197.255.248.0/21,
IPv6	2001:42d0::/32, 2001:43f8:0040::/48, 2001:43f8:0090::/48, 2001:43f8:00d0::/48, 2001:43f8:0110::/48, 2001:43f8:0120::/48, 2c0f:fe00::/32,
ASNum	33764, 37177, 37181, 37278, 327681,
CRL Distribution Point	rsync://rpki.afrinic.net/repository/984C3E6C913511DF9423B0C4AD001804/s8JRYwJxUOb-rSbfN1Jg5Piwqro.crl
Policies	critical 1.3.6.1.5.5.7.14.2
Basic Constraints	critical TRUE
Key Usage	critical Certificate Signing, CRL Signing

Add **Control** to the two shortcuts above to place the screen shot on the clipboard instead of

afrinic.net   https://beta.afrinic.net/resources/rpki/roa/view?id=28   Google

isited ▾   Getting Started   Latest Headlines 🔊   Features/DNSSEC – ...   IETF Journal–IETF–K...   Whois v3 object tem...   The Dell Online Stor...   draft–change 32bit ...   RIPE Databas

rican Network Information C... ⊗ | 🍎   Apple – Start   ⊗ | 📄   African Network Information C... ⊗ | +

AfriN

| Home | Control Panel | My Account | Billing | **Resources** | Help & Support |

AS Numbers   IPv4 Resources   IPv6 Resources   Reverse

ation   Resource Certification   [Sign-Out]

a Alain Patrick @ African Network Information Center - (AfriNIC Ltd)

re here: Home > Resources > Resource Certification > roa > View ROA

-- Quick Links --   Jump

Whois

Advanced Options

Calendar

November   2010

Mon	Tue	Wed	Thu	Fri	Sat
1	2	3	4	5	6
8	9	10	11	12	13
15	16	17	18	19	20
22	23	24	25	26	27
29	30				

View ROA

id	28
Name	AFRINIC
revoked	No
product-url	rsync://rpki.afrinic.net/member_repository/F4D17C32914011DFA116BB5E4DC4681B /01244A70981A11DFB75CC6212EE1294A.roa
as-number	17652
not-before	2010-07-25 14:25:50
not-after	2011-07-25 14:25:50
ipv4	196.1.0.0/24

(Revoke)

5. Add **Control** to the two shortcuts above to place the screen shot on the clipboard instead of

Photoshop Elements 9

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

Questions ?