
RPKI deployment at AfriNIC

Status Update

AfriNIC-13
Johannesburg, 24/11/2010

Alain P. AINA
RPKI Project Manager/Spokesman

Laban MWANGI
Project member/Deputy Speaker

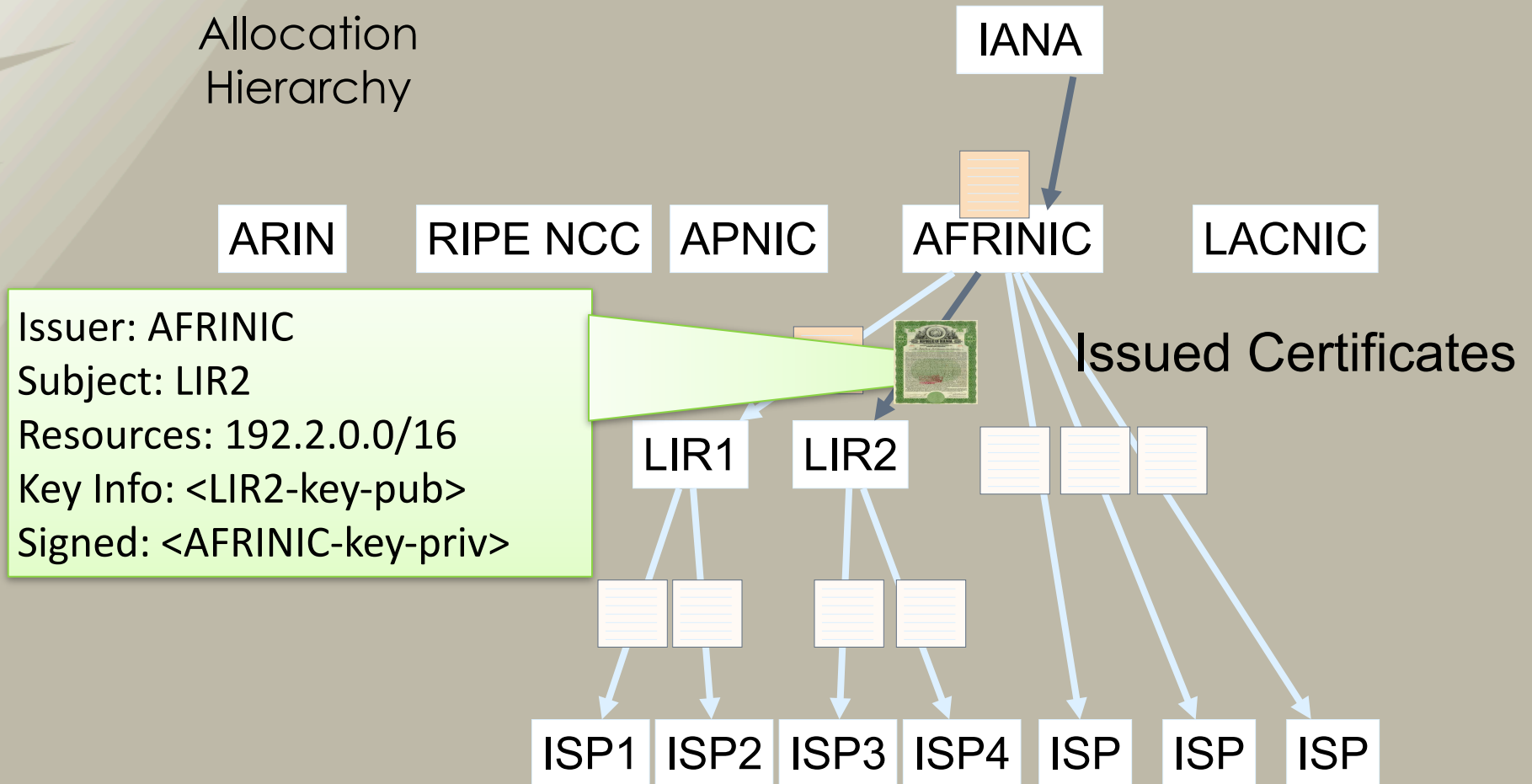


Motivations for RPKI

- **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

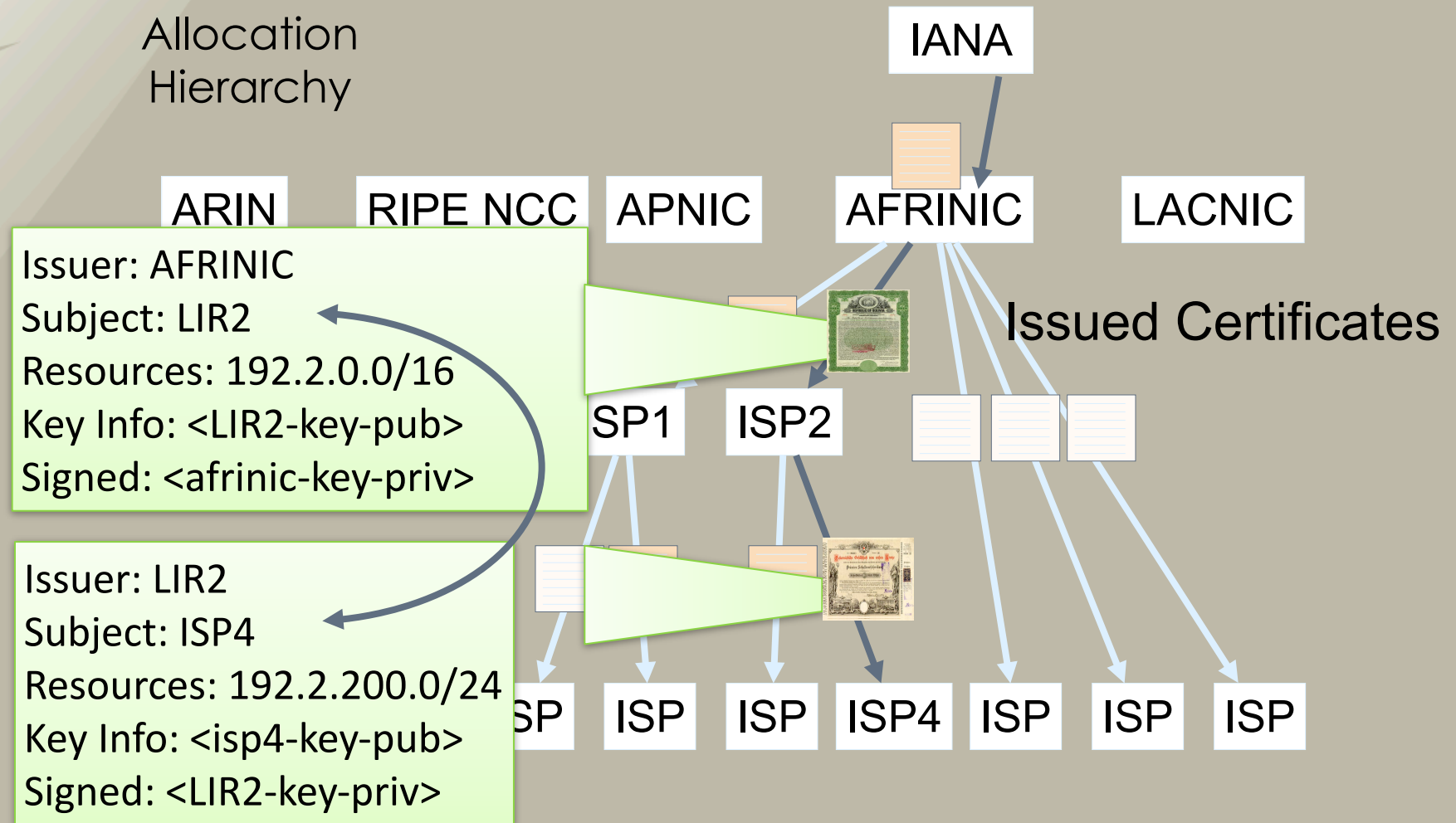
Resource Certificates

Resource
Allocation
Hierarchy



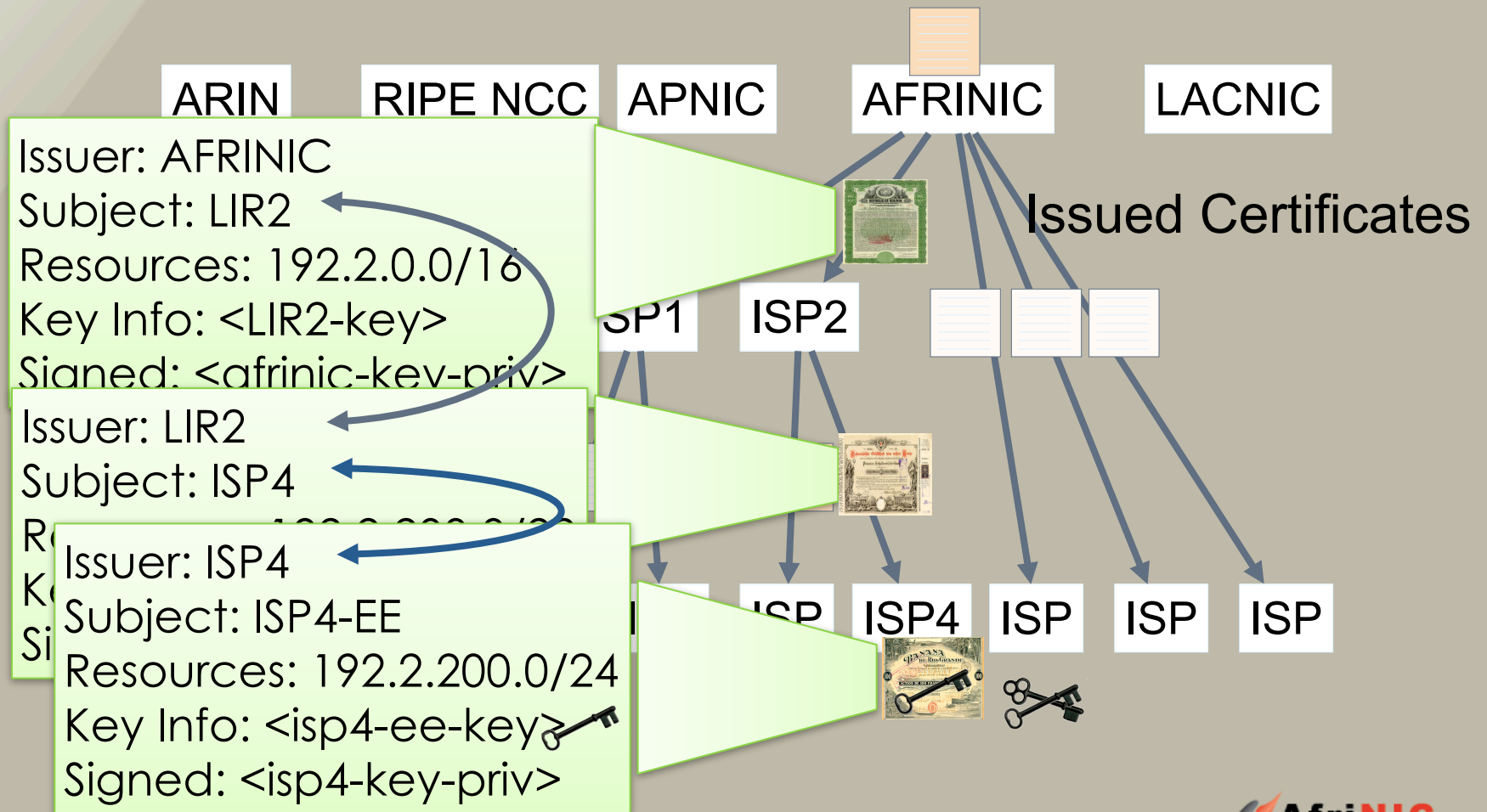
Resource Certificates

Resource
Allocation
Hierarchy



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 Roadmap to Production

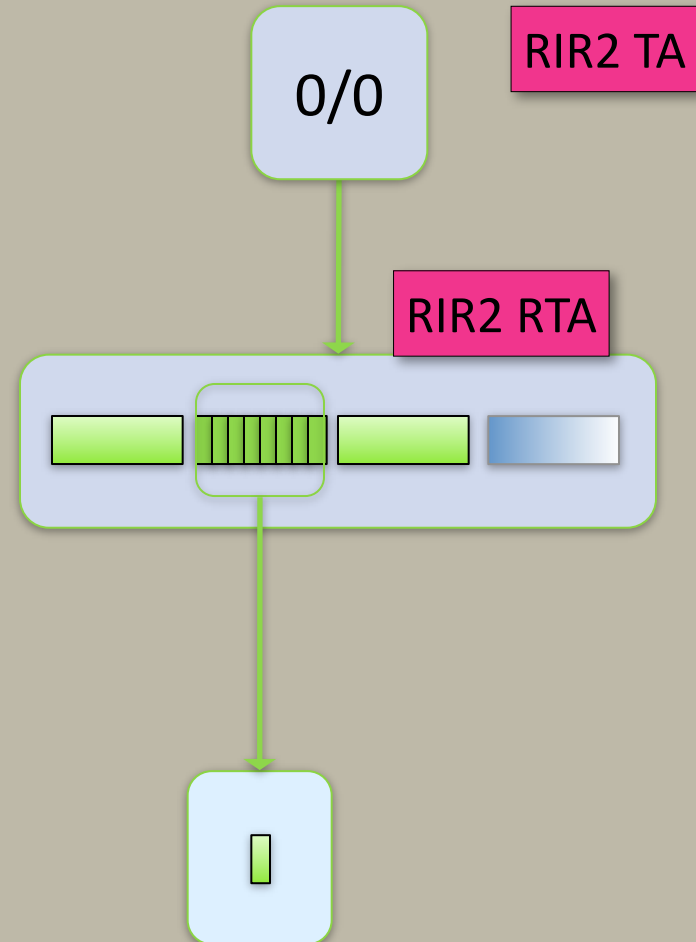
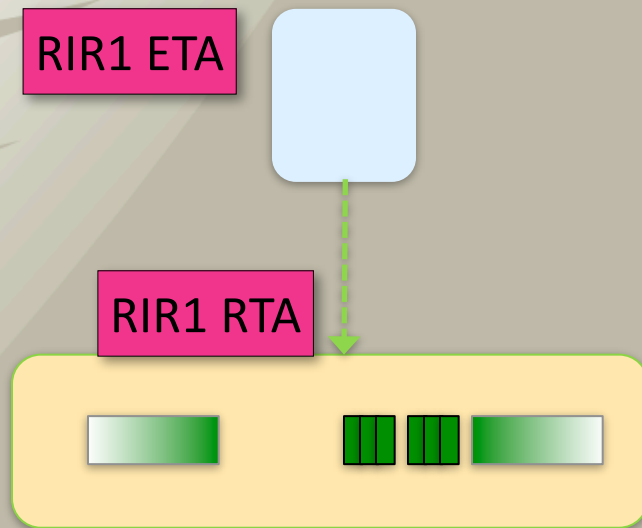
– 4 Phases by the NRO

- **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

Phase 1: Pilot

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

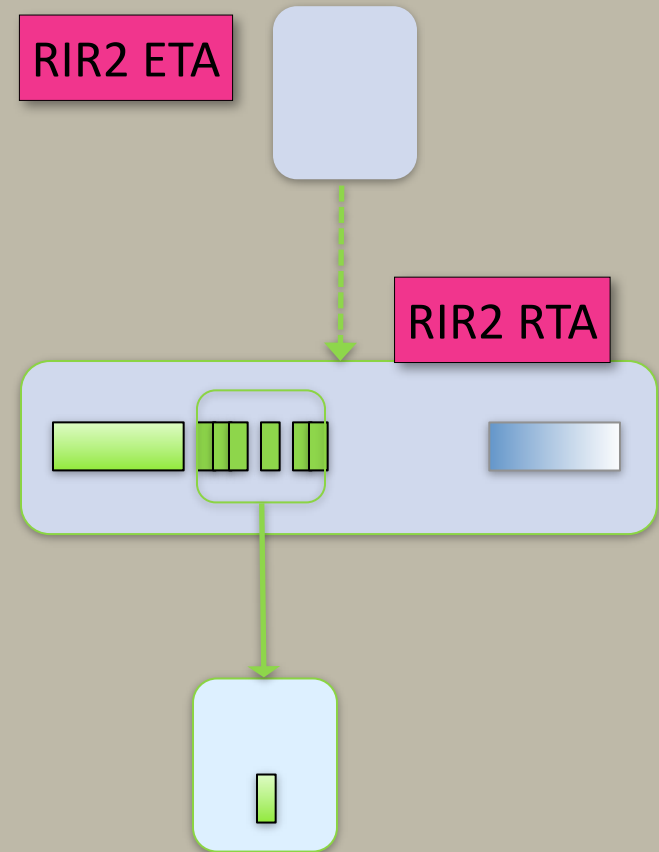
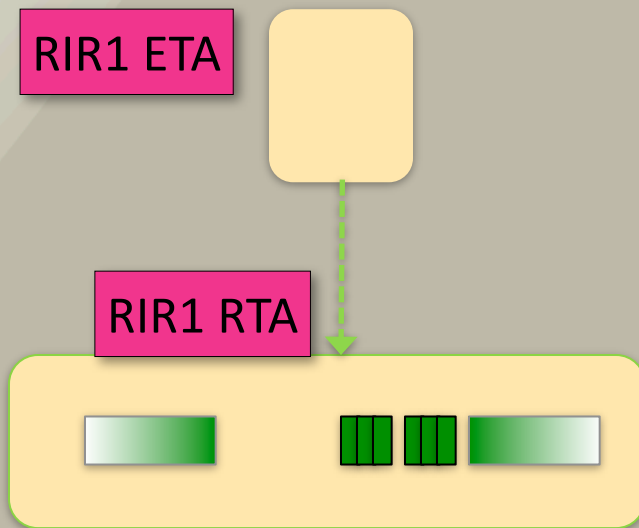
Phase 1: Pilot



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

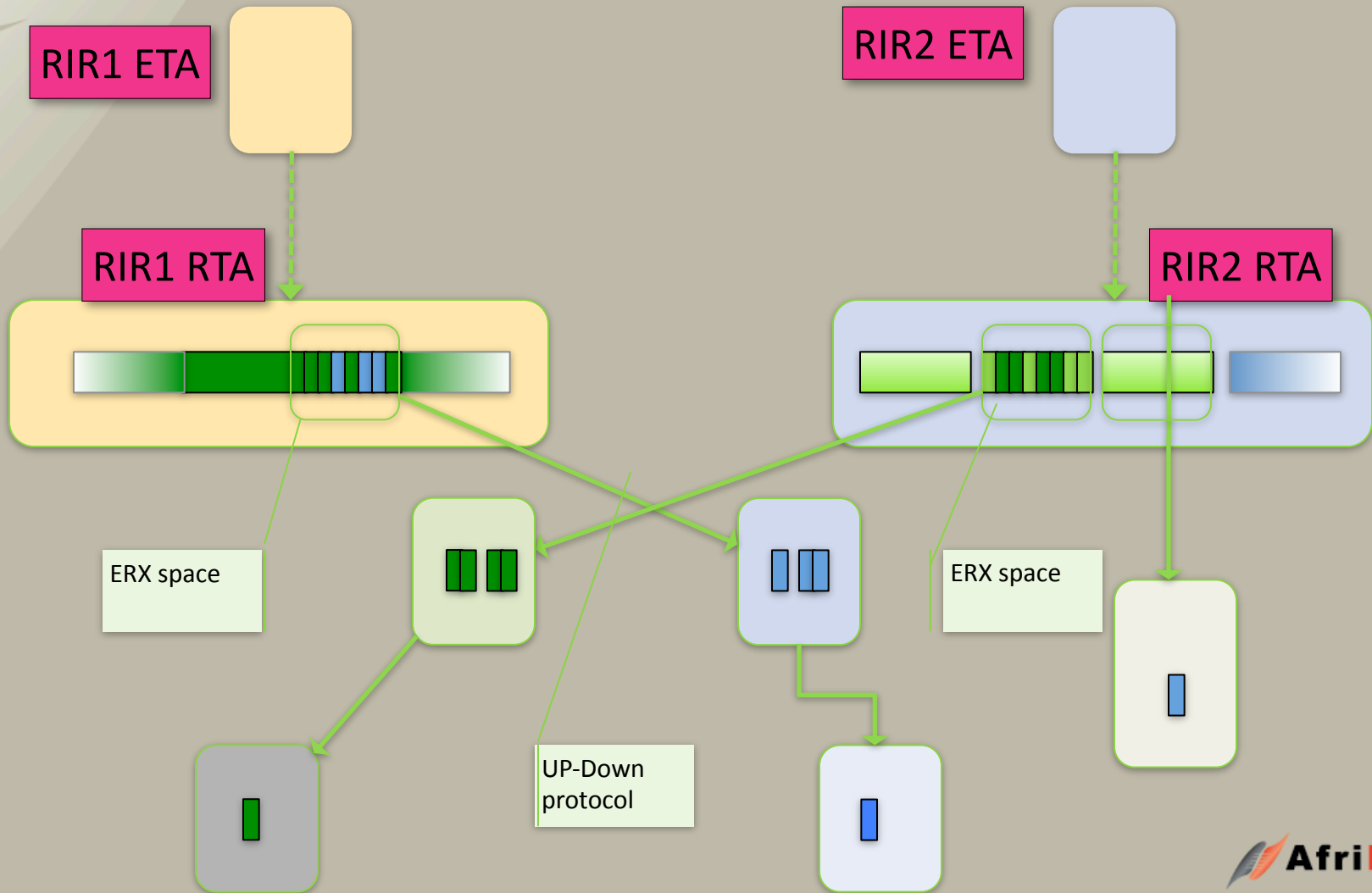
Phase 2: Initial Production



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

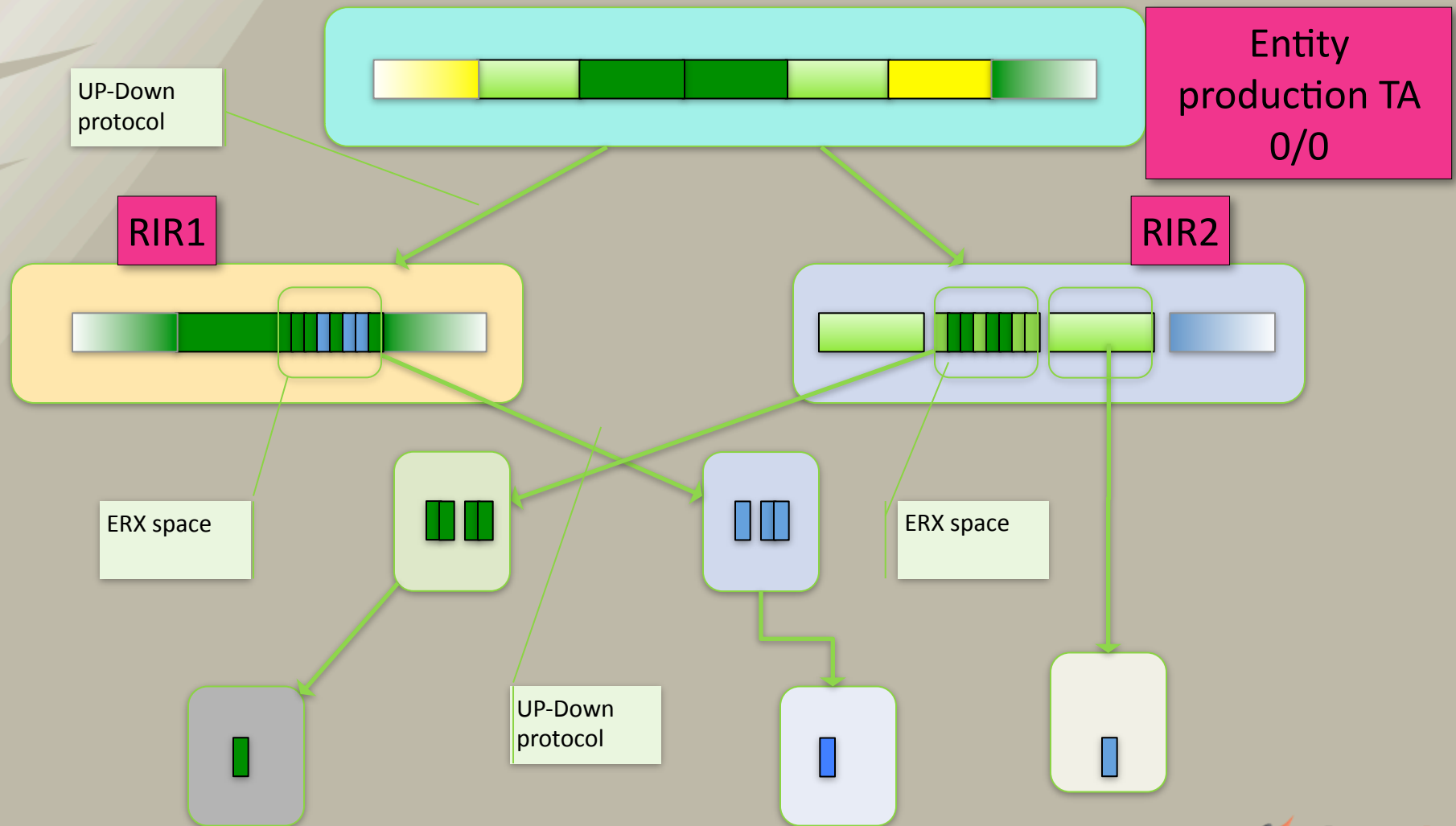
Phase 3: Global Consistency



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

Phase 4: Single TA



RIR Deployment Status

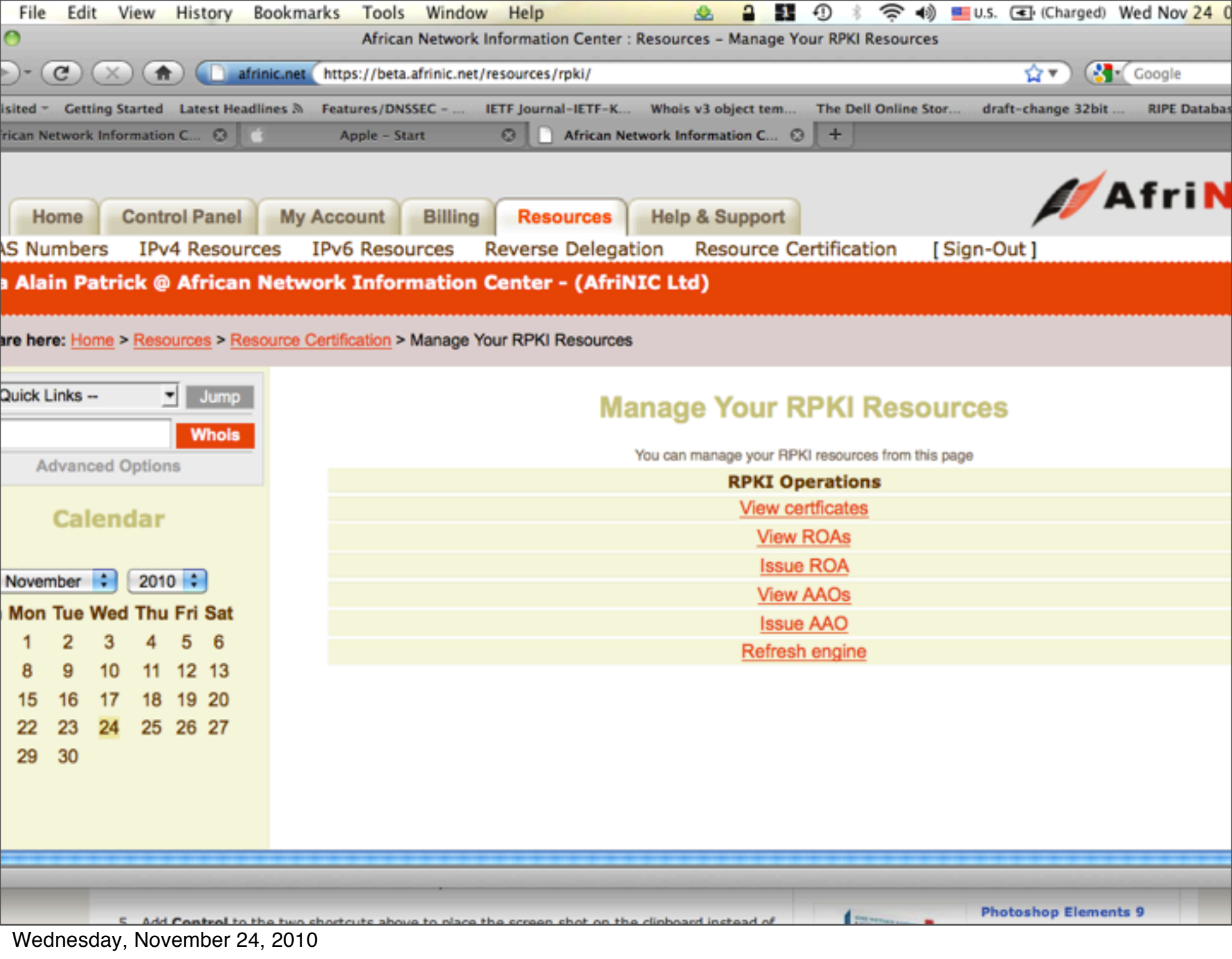
- Each RIR has completed Phase 1
- Working on Phase 2

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>
- Under intensive internal testings

AFRINIC's RPKI System

- Statement (CPS) is under review
 - Only those who have a contractual relationship (RSA) can participate
 - Certificate Expiration Dates ???
 - Tied to RSA ?
 - » Certs expired on 31/12
 - » Certs renewed with overlap to avoid service interruption !!!
- SLA: which and how ?



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

FileEditViewHistoryBookmarksToolsWindowHelp

African Network Information Center : Resources - View ROA

afrenic.nethttps://beta.afrenic.net/resources/rpki/roa/view?id=28

Google

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

African Network Information C... Apple - Start African Network Information C...

HomeControl PanelMy AccountBillingResourcesHelp & Support

AS NumbersIPv4 ResourcesIPv6 ResourcesReverse

ationResource Certification[Sign-Out]

Alain Patrick @ African Network Information Center - (AfrNIC Ltd)

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

Quick Links -- Jump

Whols

Advanced Options

Calendar

November2010

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

id28

NameAFRINIC

revokedNo

product-urlrsync://rpki.afrenic.net/member_repository/F4D17C32914011DFA116BB5E4DC4681B/01244A70981A11DFB75CC6212EE1294A.roa

as-number17652

not-before2010-07-25 14:25:50

not-after2011-07-25 14:25:50

ipv4196.1.0.0/24

Revoke

5. Add Control to the two shortcuts above to place the screen shot on the clipboard instead of Photoshop Elements 9

Firefox File Edit View History Bookmarks Tools Window Help



Index of /

afrrinic.net https://rpki.afrrinic.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.afrrinic.net Port 443

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

AFRINIC's Roadmap for RPKI

- **End of December 2010** – Tests open to our community on our "initial production system"
- **March 2011**- Hosted RPKI system in production
- **July 2011** - RPKI services via Up/Down protocol for ISP subdelegations
- **Oct 2011** – Implement inter-RIR Transfers within RPKI System



RIR Challenges

- Solidified CPS
 - Need to coordinate with the other RIR's
- Matching code against changing standards
 - Everything based on I-Ds from SIDR WG
 - TLS being dropped
 - New Trust Anchor Format
- Mechanics of inter-RIR transfers not yet settled
- Lots of learning(Tech. admin. Legal...)

Questions ?