RPKI deployment at AfriNIC Status Update

AfriNIC-15
Yaounde,11/23/2011

Alain P. AINA
RPKI Project Manager/Spokesman

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

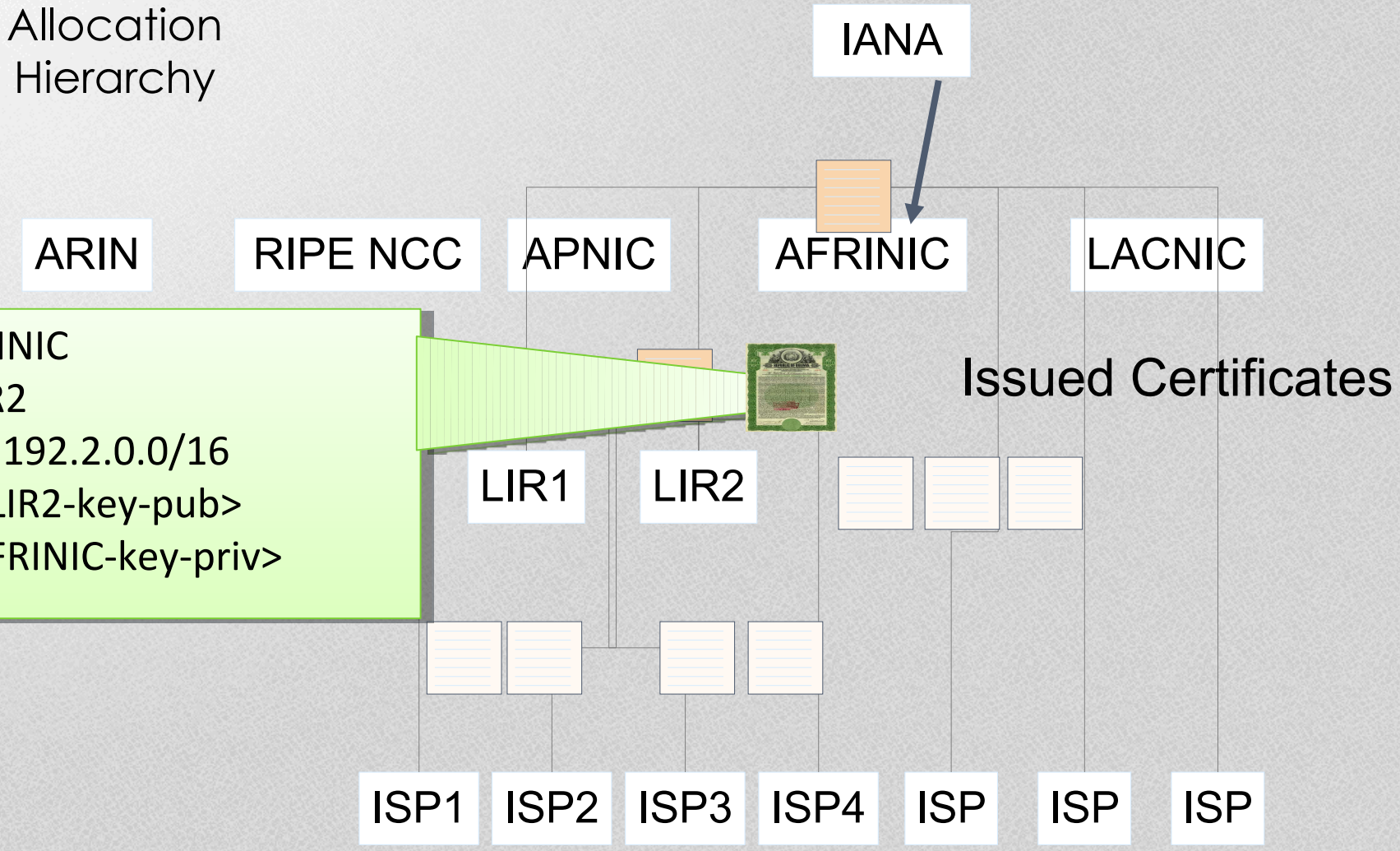
Resource Public Key Infrastructure(RPKI) is a PKI based on the Internet resources management hierarchy and under which X509 certificates with RFC 3779 extensions and other signed objects are published and bound together in an verifiable way.

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

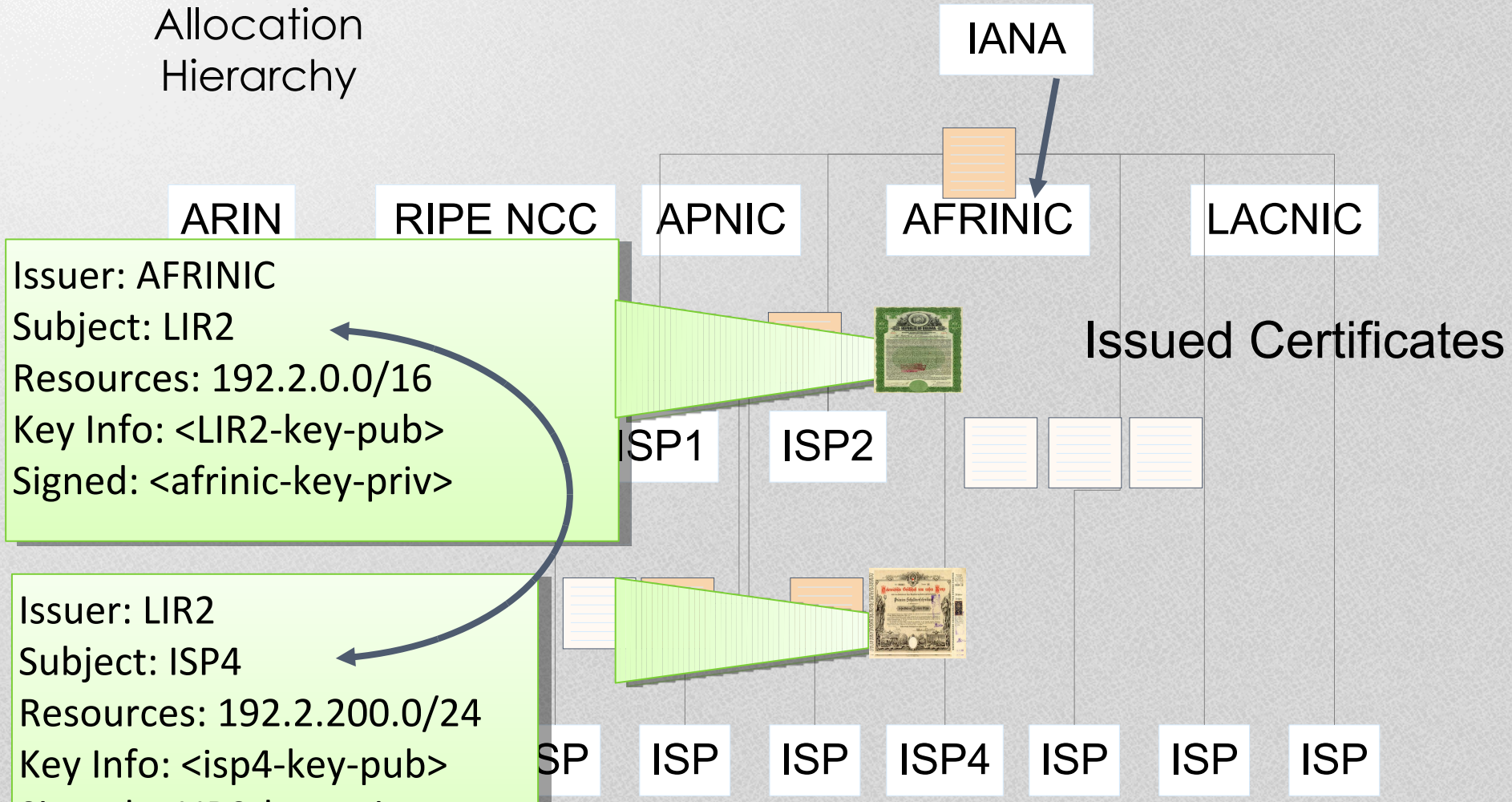
Resource Certificates

Resource Allocation Hierarchy



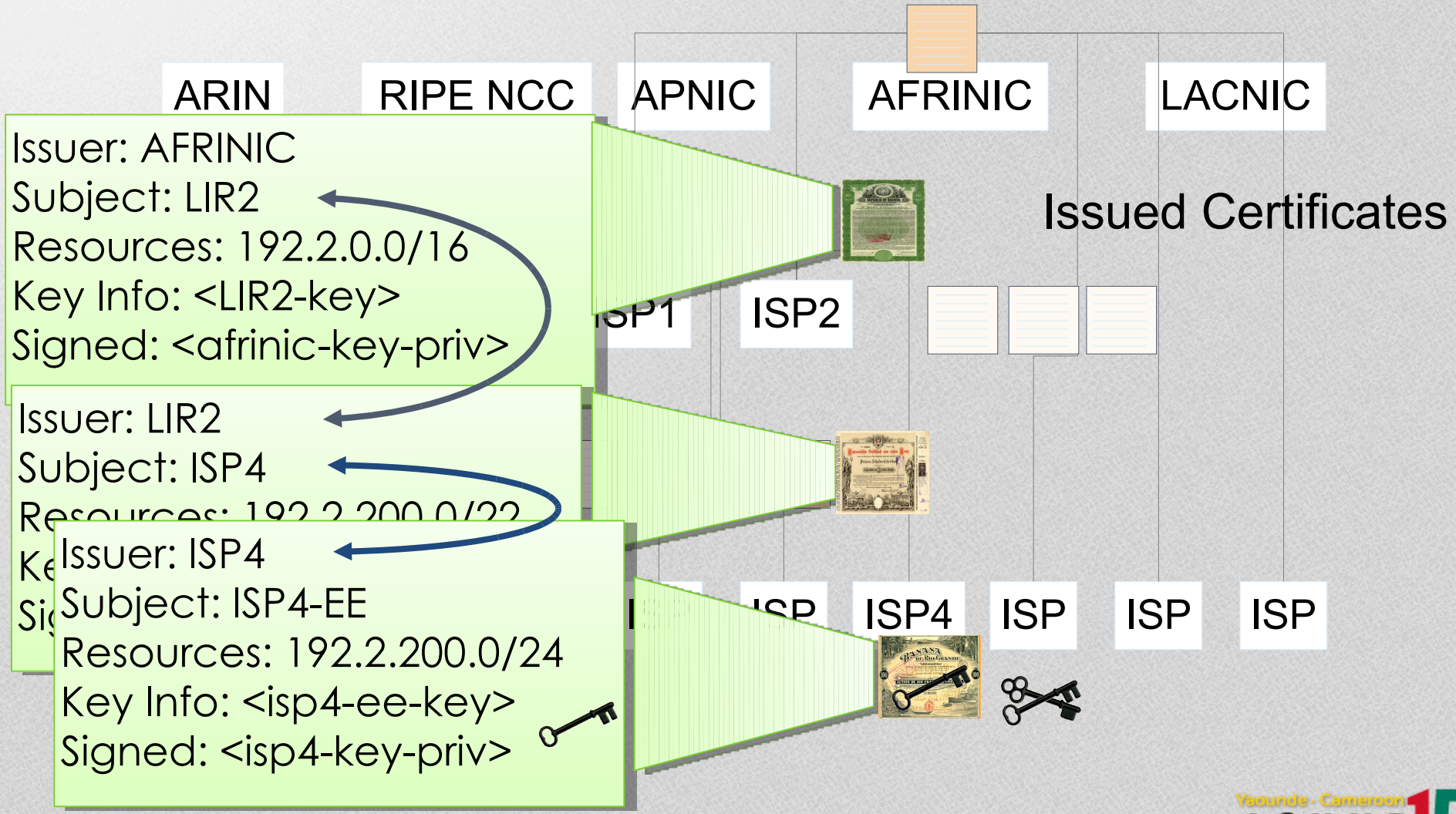
Resource Certificates

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 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
  - TA
  - CP & consistent CPS's
- Inter-RIR transfers handled manually

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 4: Single TA

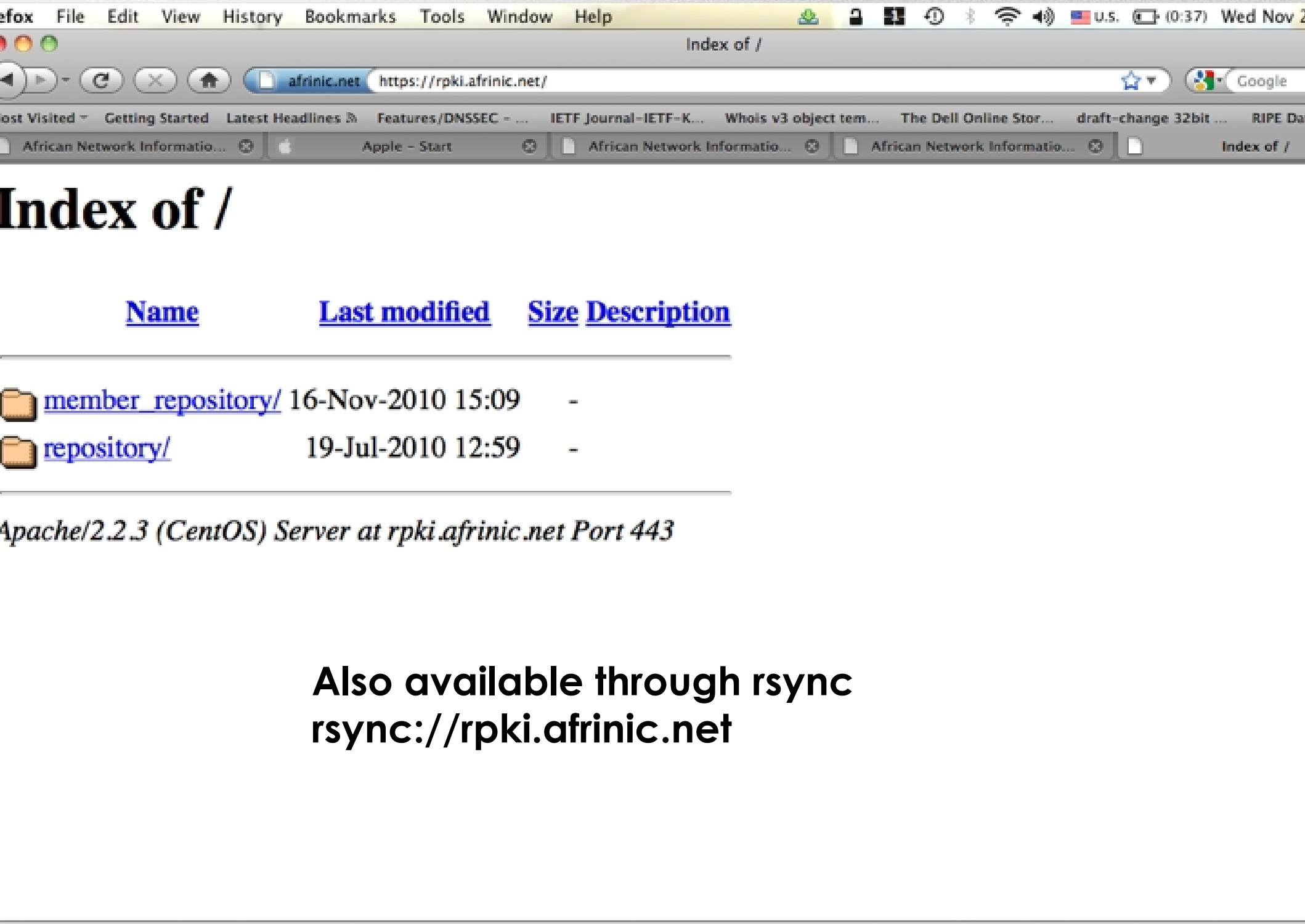
- One Single TA
  - May be a natural 0/0
- Standard
  - Resource Certificates
  - Repositories
  - Up-Down protocol
  - CP & consistent CPS's
- Changes to the global registry and transfers can be automated

AfriNIC'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

RIR Deployment Status

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


efox File Edit View History Bookmarks Tools Window Help
Wed Nov
Index of /
afrinic.net
https://rpki.afrinic.net/
Google
ost Visited
Getting Started
Latest Headlines
Features/DNSSEC - ...
IETF Journal-IETF-K...
Whois v3 object tem...
The Dell Online Stor...
draft-change 32bit ...
African Network Informatio...
Apple - Start
African Network Informatio...
African Network Informatio...
Index of /
Index of /
Name
Last modified
Size
Description
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
one
transfers can be automated

Questions ?