

---

# Resource Certification

## What it means for LIRs

---

Alain P. AINA

Special 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.

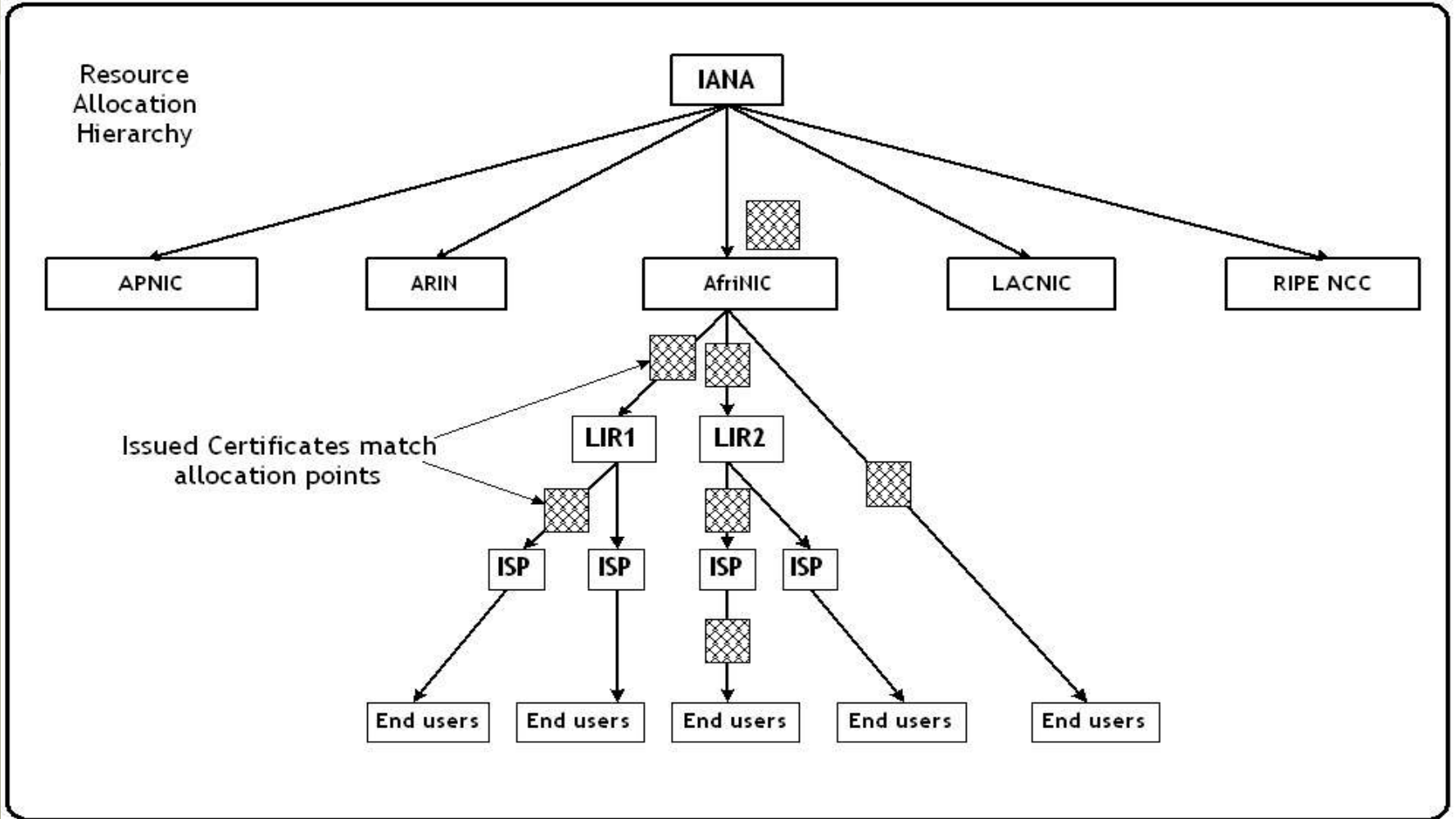
---

# Motivations

---

- Facilitate a 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*

# Overview



---

# Overview

---

## A RPKI Certificate

Pointer to issuer (AIA):	rsync://.../....cer
Pointer to own repository (SIA):	rsync://.../.../
Public Key information :	...
Issuer name :	AfriNIC
Subject name :	Agtk4bx41rFhtQ
Resources :	41 / 16
	AS65540

Issuer's signature



**THIS IS NOT AN IDENTITY  
CERTIFICATE**

---

# Use Cases

---

- ROAs - against hijacks
- Enabling S\*BGP
- Customer sign-up
- Resources transfers
- RPSLSIG
- ROA2RPSL ?
- Bogon filtering – BOAs?

More to come :-)

---

# Use Cases: ROA

---

## ROA – Route Origination Authorization

Using my certificate covering a prefix, I can formally, verifiably authorize an AS to announce that prefix

- Can be useful for constructing route filters
- Could be used by S\*BGPAs

# Use Cases: ROA

## ROA – Route Origination Authorization

Prefix:	192.168.0.0/16
Authorised AS:	AS65540
Signer Certificate :	rsync://.../....cer
Valid from :	2008-05-01T08:00:00Z
Valid until :	2008-05-01T08:00:00Z

Prefix holder's signature

### ROA validity chain

AfriNIC

Certificate

LIR

Certificate

Customer

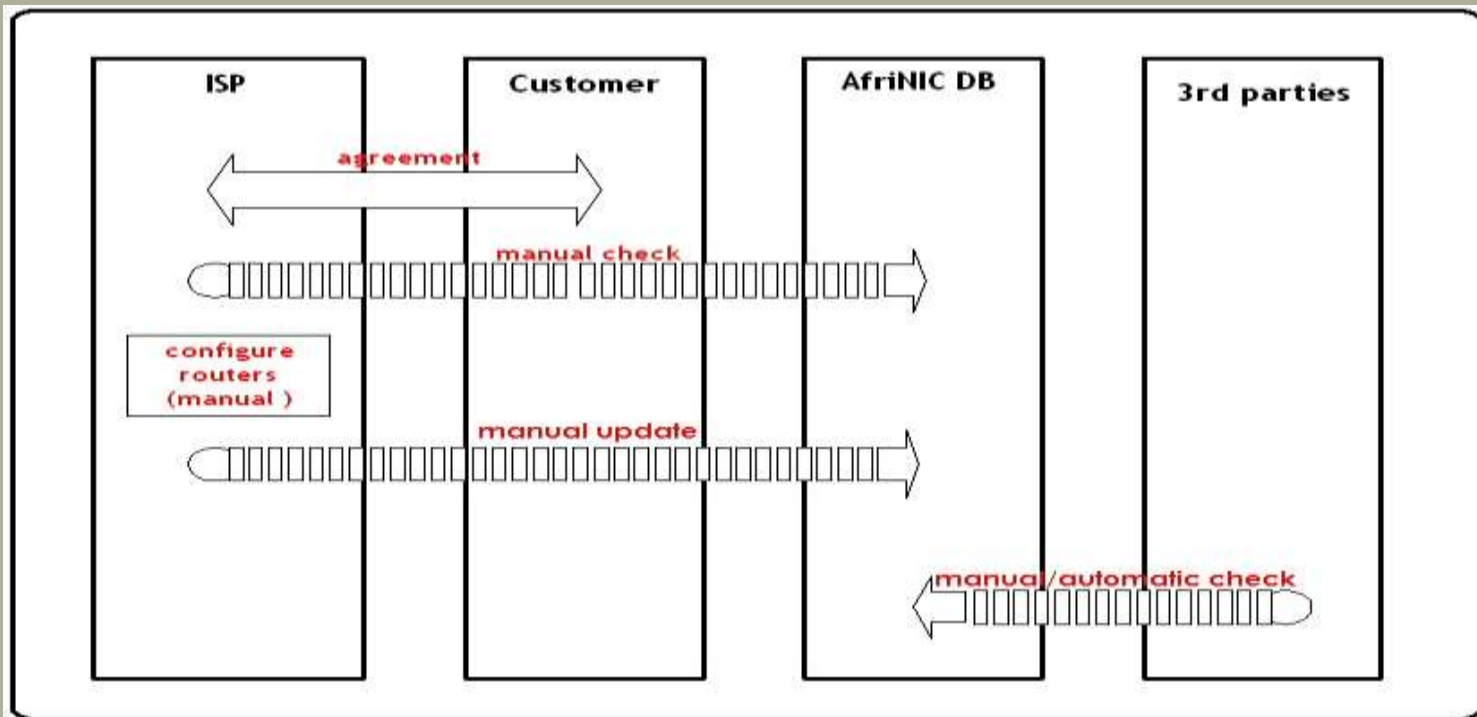
Certificate

ROA

# Use Cases: Customer Sign-up

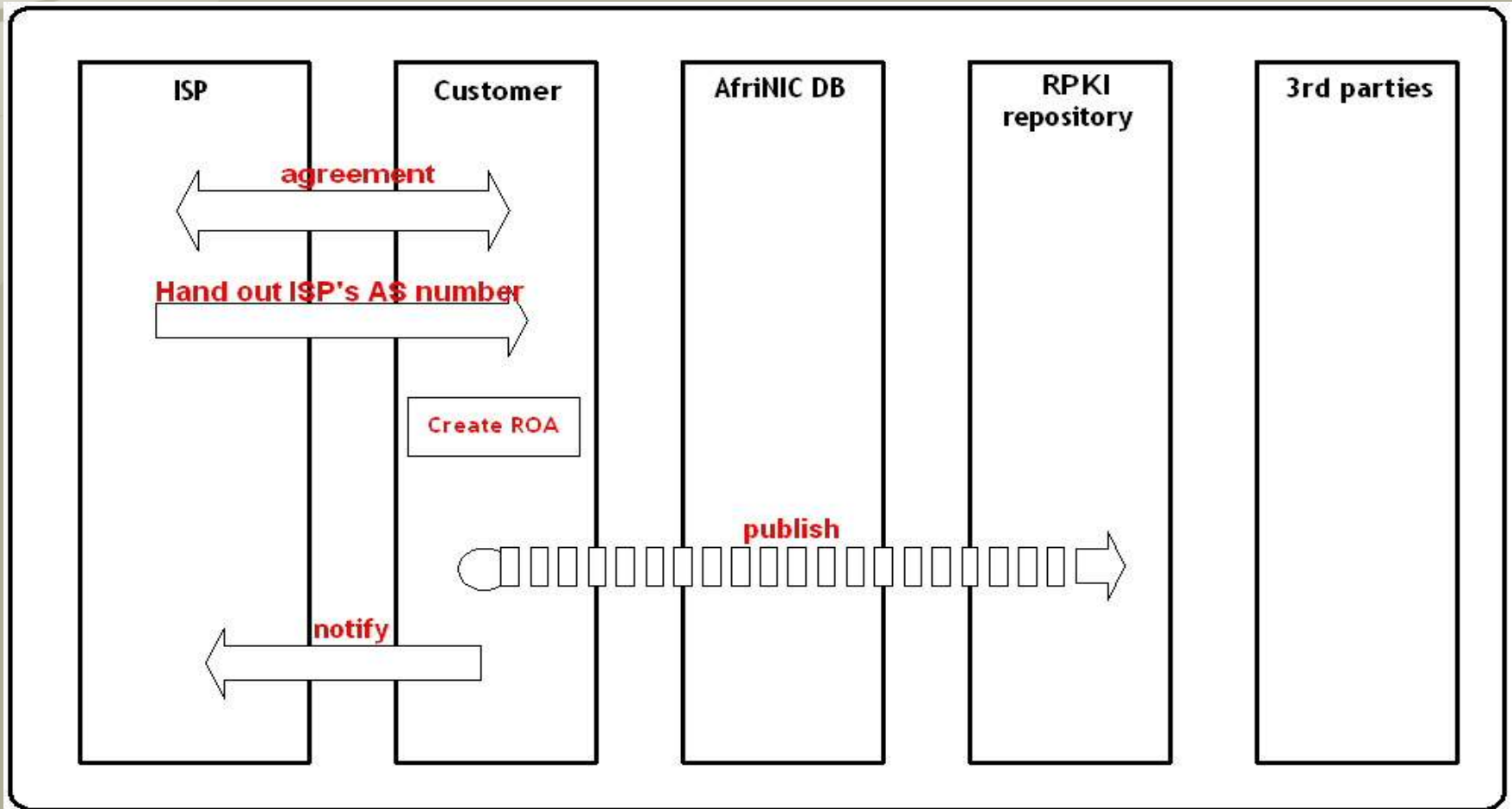
Without RPKI

How do you verify their claim over a resource?



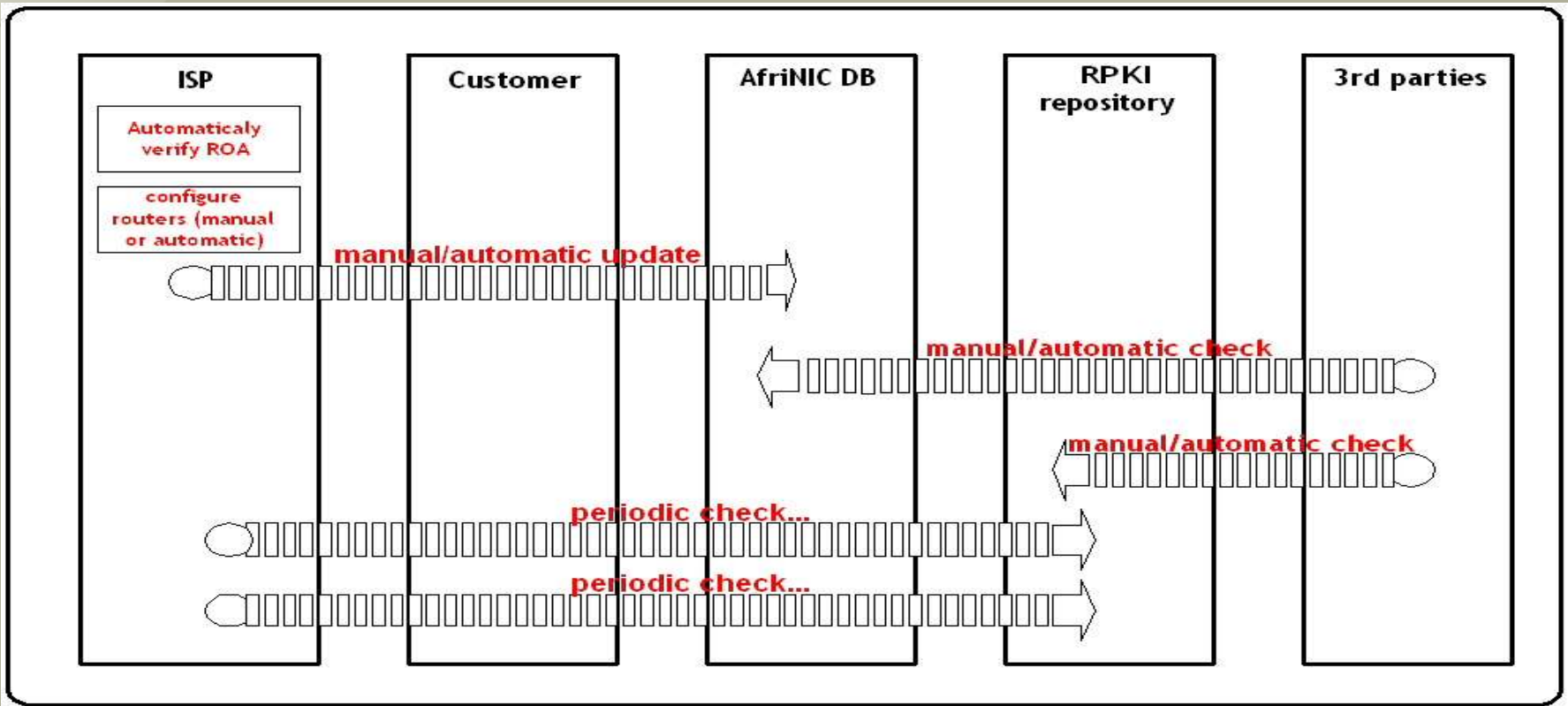
# Use Cases: Customer sign-up

## With RPKI



# Use Cases: Customer sign-up (cont'd)

## With RPKI



---

# Use Cases: RPSLSIG

---

## Combining RPKI and RPSL: RPSL Signatures

- Use RPKI to sign RPSL objects by extending RPSL syntax
- It could raise the trust level of RPSL data by providing “object security” as an addition

For example:

*Prefix and AS holder both sign a route object, thereby expressing their agreement on it.*

---

# Use Cases: RPSLSIG

---

Route: 192.0.2.0/24

descr: GroupNet and ISP1

origin: AS65536

mnt-by: GroupNet-MNT

signature: v=1;c=rsync://.../....cer; m=sha1- rsa;t=2009-03-01T10:11:01T;a=route+descr+origin+mnt-by;b=324kjndfg9083GAD4sEW32.

signature: v=1;c=rsync://.../....cer; m=sha1- rsa;t=2009-03-02T11:11:01T;a=route+descr+origin+mnt- by;b=9ds3D4sW3234tj11wdhuon...

source: AFRINIC

---

# Participating in the RPKI

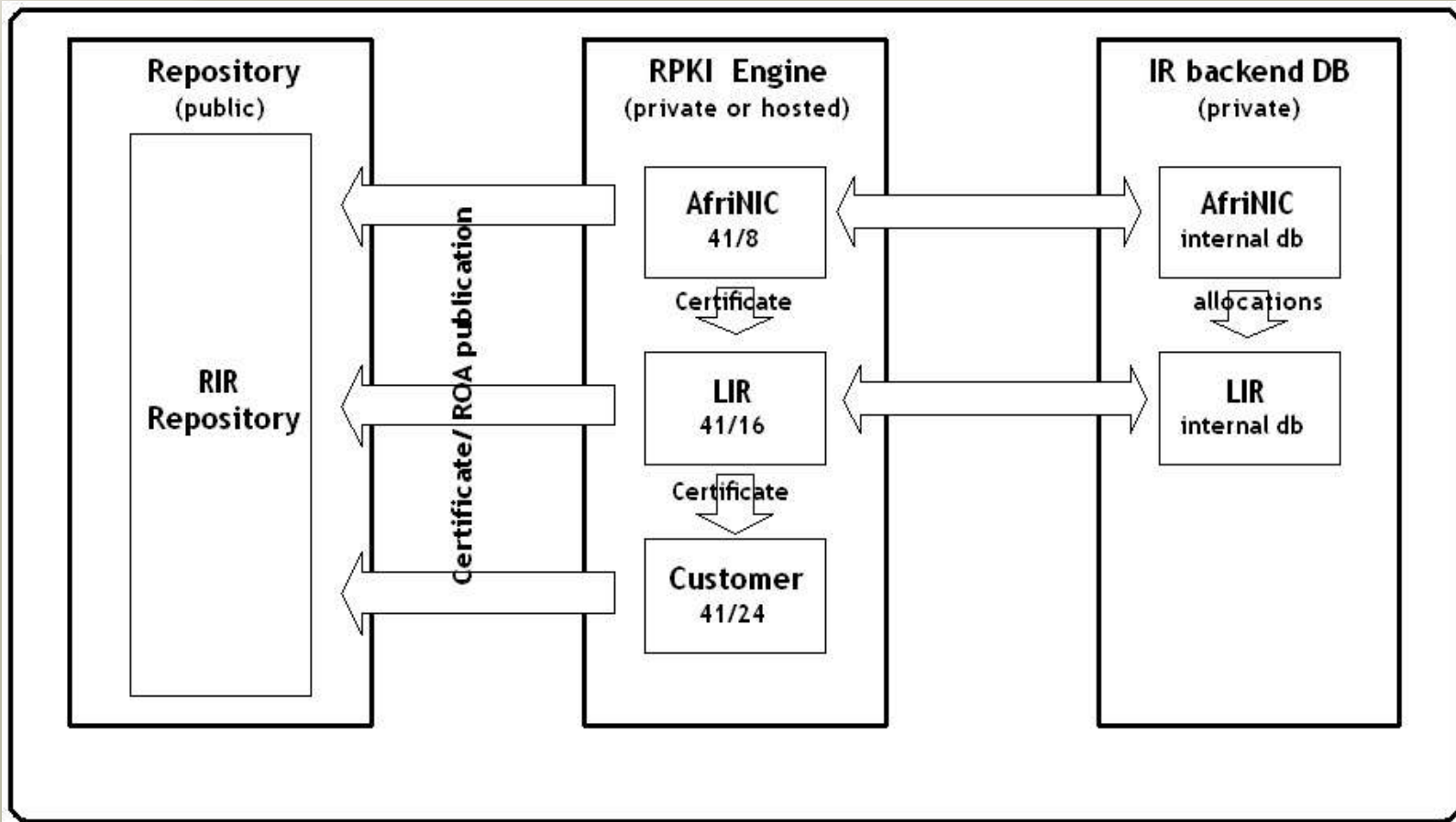
---

Internet Registries(RIR/LIR/ISP) can:

- Receive their certificates from their “upstreams”
- Issue certificates to their clients or themselves:  
*End Entities Certificate*
- Sign data with operative content using their own  
Certificates

# Participating in the RPKI

## Enter the RPKI Engine



---

# Participating in the RPKI

---

To participate, an IR needs:

- RPKIE software and an infrastructure to run it
- On the higher levels: Hardware Security Module(s)
- Good back-end database of resource delegations
- Some Mandatory documents for a PKI:
  - *Certificate Policy (CP)*
  - *Certification Practice Statement (CPS)*

---

# Services for the RPKI

---

## Intended AfriNIC services for LIRs:

- Certify LIR resources using the AfriNIC own 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 LIRs 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*

---

# Services for the RPKI

---

## Potential services:

- Central cache for certificates (repository collection)
- Certificate validation
- Object validation
- Repository service
- Others?

# Trust Anchors for RPKI: Which root CAs ?

- TA choice is the Relying Party's decision
- For the RPKI, RIRs seems to be a natural choice  
*But just as every IRs, they will only certify what they allocate/assign*
- Possible use of multiple TAs
- IANA can also be a single (or an additional) TA
- The NRO statement of the RPKI TA

<http://www.nro.net/news/nro-declaration-rpki.html>

Questions ???

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

A resource certification portal soon