Certification More Tangible

RIPE Certification Task Force

Nigel Titley, Trudy Prins, Oleg Muravskiy

RIPE 56, May 2008

Drivers

- RIR's are implementing a solution to certify resources
  - APNIC and ARIN are implementing an RPKI engine
- RIPE NCC has the task to uphold principles
  - Uniqueness
- Enhancing Registration Processes
- Improve and increase robustness of transfer mechanism
  - Increase in IPv4 transfers could turn into routing chaos

Story so Far (1/3)

- November 2006 - RIPE 53
  - Goal(s): Proposal to establish the task force.
- February 2007 - Initial meeting
  - Goal(s): Understanding the context
  - Results:
    - Discussed high level view point
    - Acknowledged the complexity and impact of the project
    - Demonstration on technical feasibility
    - Consensus on moving forward with the Certification project
  - Plan:
    - De-complex the project by defining impacted areas
    - Assess knowledge
    - Increase understanding by external stakeholders (other than the CA-TF)
    - Progress and track technical standards setting and theory

Story so Far (2/3)

- May 2007 – RIPE 54
  - Goal(s):
    - Publish a progress report and discuss the outcomes of the work done so far
  - Results:
    - Policy area (greenish - understanding of issue areas)
    - Services area (amber - understanding of internal processes needed)
    - Technical area (amber - high level knowledge)
    - RIR wide area (amber - high level knowledge)
    - Application area (red - what is the value for our membership / uptake)
  - Plan: Focus on technical feasibility and application of Certificates
- October 2007 – RIPE 55
  - Goal(s): Report on progress to task force
  - Results: Discussion on high level prevent us moving ahead
  - Plan: Develop tangible applications (based on business cases), technical implementation will not be the blocking issue

Story so far 3/3

- March 2008 – CA TF Meeting
  - Goals:
    - Discuss progress and current status,
    - Discuss white-papers describing applications and values,
    - Prioritise next efforts (towards RIPE 56)
    - Define needed Policy proposals & discussion
    - High level planning and goals for RIPE 56
  - Results:
    - Consensus on business value of Certification for the wider community and membership
    - Consensus on “Go” for next phase (pre-production testing phase)
  - Plan:
    - Announce pre-production version at RIPE 56
    - Initial Provisioning Policy Proposal

Added value

- Certificates can be the inter-regional exchange standard between RIR's
- Facilitates automated provisioning
  - –easier to prove holdership than through "detective work"
  - –certified information in parseable format
- (Long term) Could help future secure routing
  - –fills need for a PKI infrastructure and trusted third party
- Support resource (IPv4, IPv6, ASN) transfers

Progress since RIPE 55 Meeting

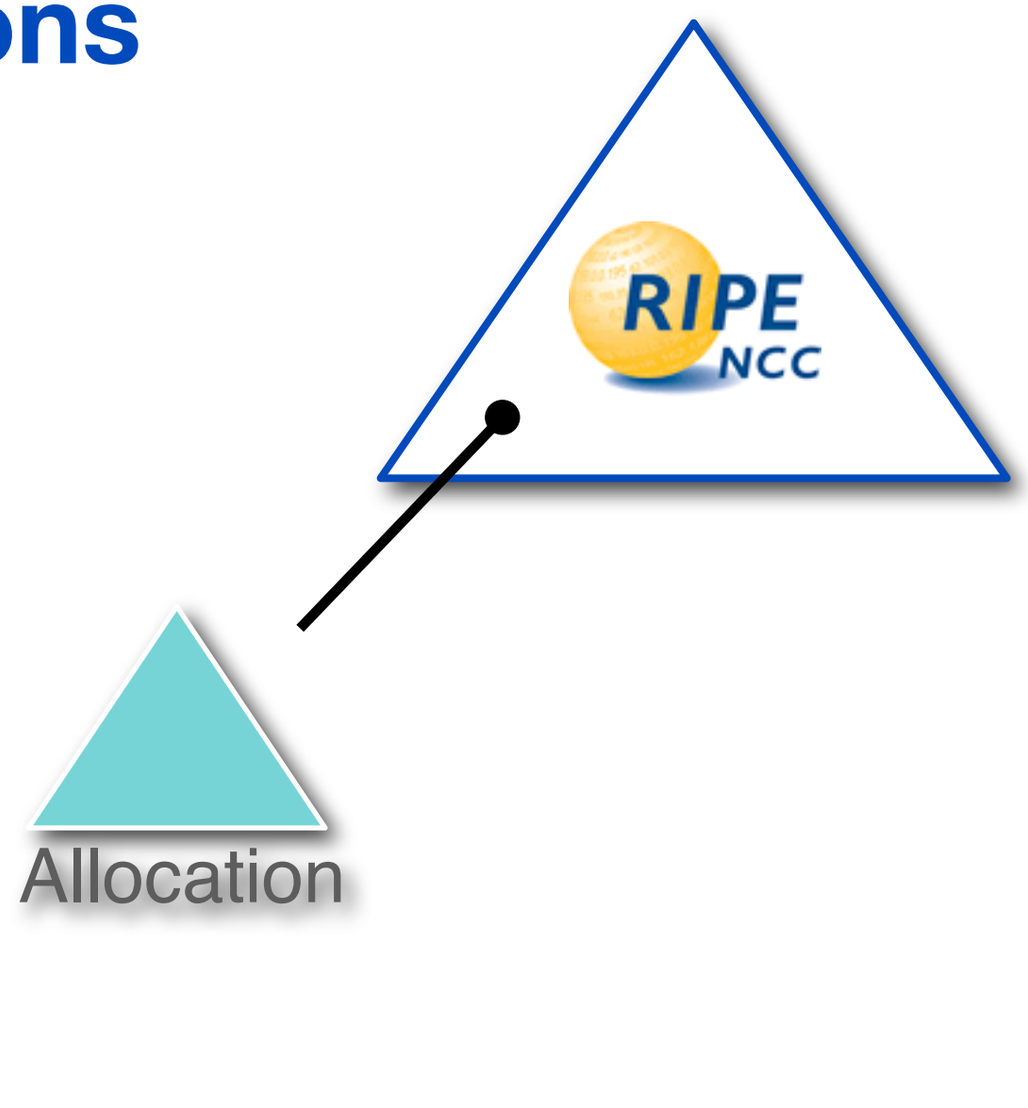
- Focus on the business value of certification for RIPE members
- Insight by starting implementation: active involvement in technical discussions
- Focus on tangibility
- Develop internal business processes to support Certification
- Closer contact with Task force
- Preparing test version of member application

What is the value of a certificate?

Certificates are not trust anchors, the registry is!

It's all about Allocations

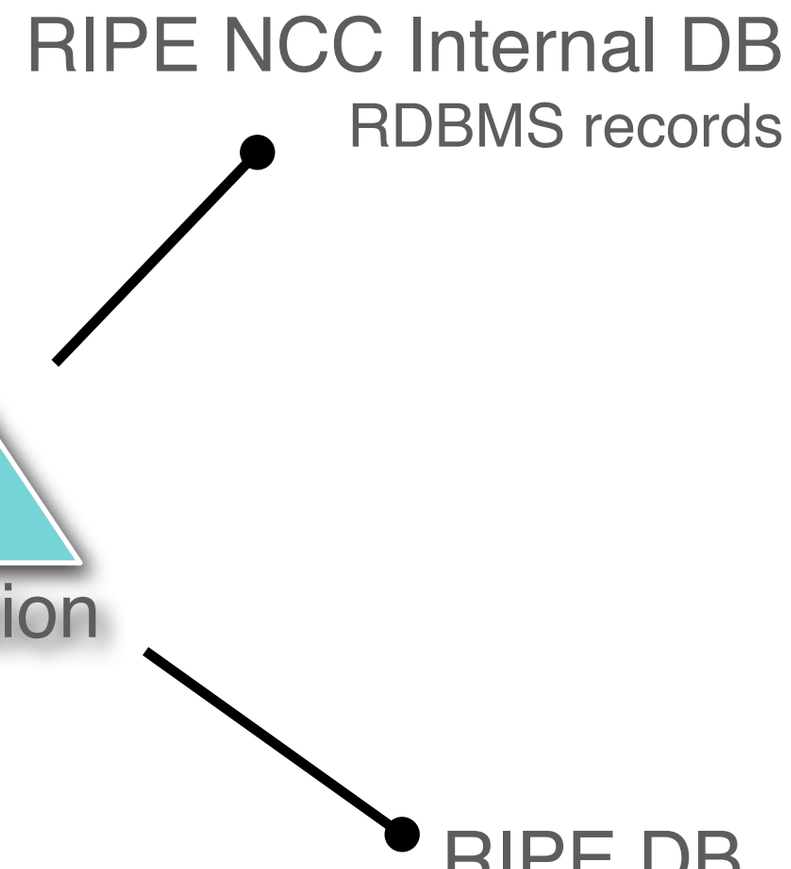
- Allocations are RIPE NCC's core concept
- Connect a party to an IP Resource



...and other kinds of parties

Certificates vs. Allocations

- A certificate is **another representation** of an allocation
- Value of certificates is **only the added value** over other representations



cer•tif•i•cate

noun |sərˈtifikit|

an official document att… n particular

- a document recordi… arriage, or death.
- a document describ… on : *certificate of immunization.*
- a document attestir… ent in a course of study or

training : *graduate certificate in information technology.*

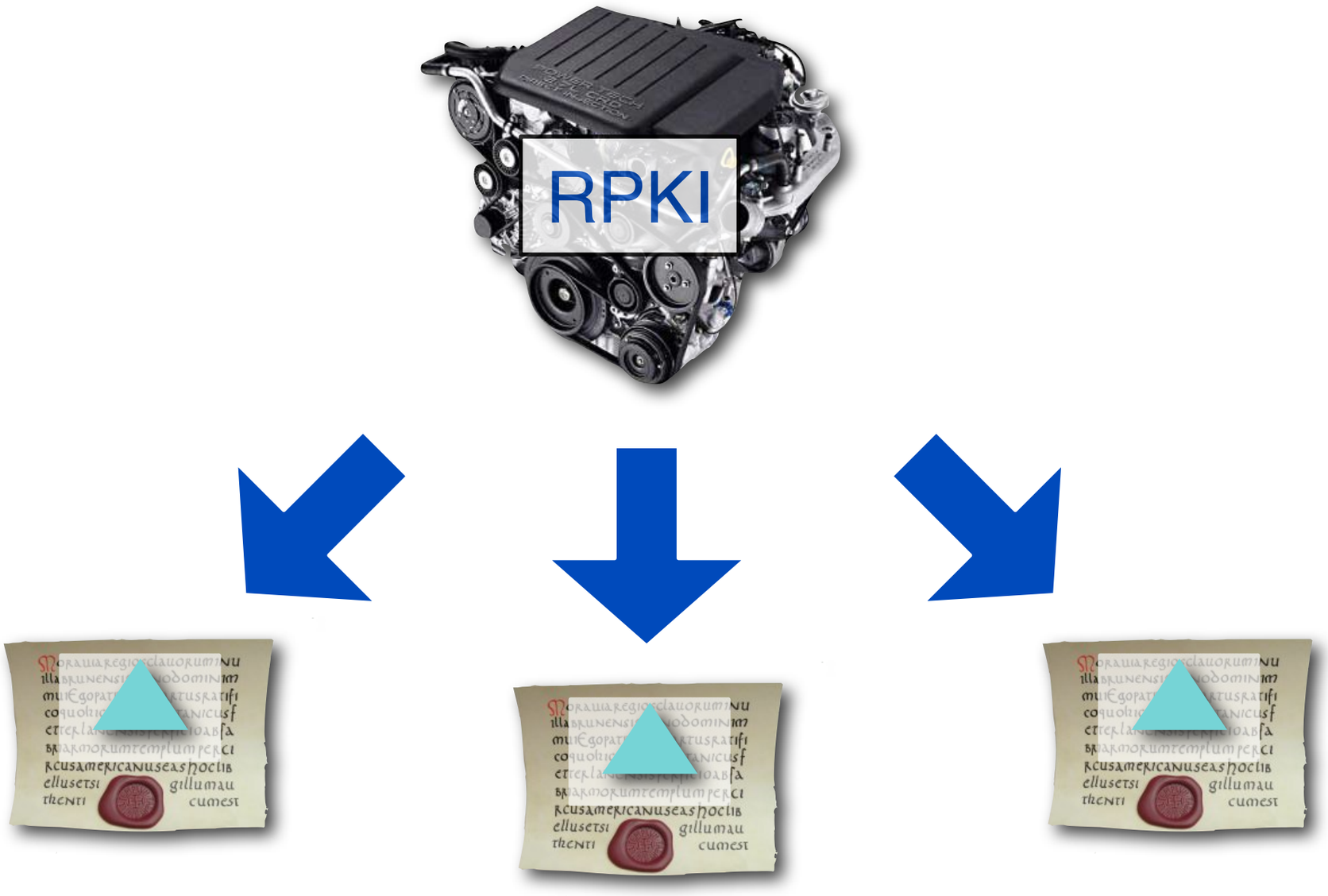
- a document attesting ~~ownership~~ of a certain item : *a stock certificate.*

holdership

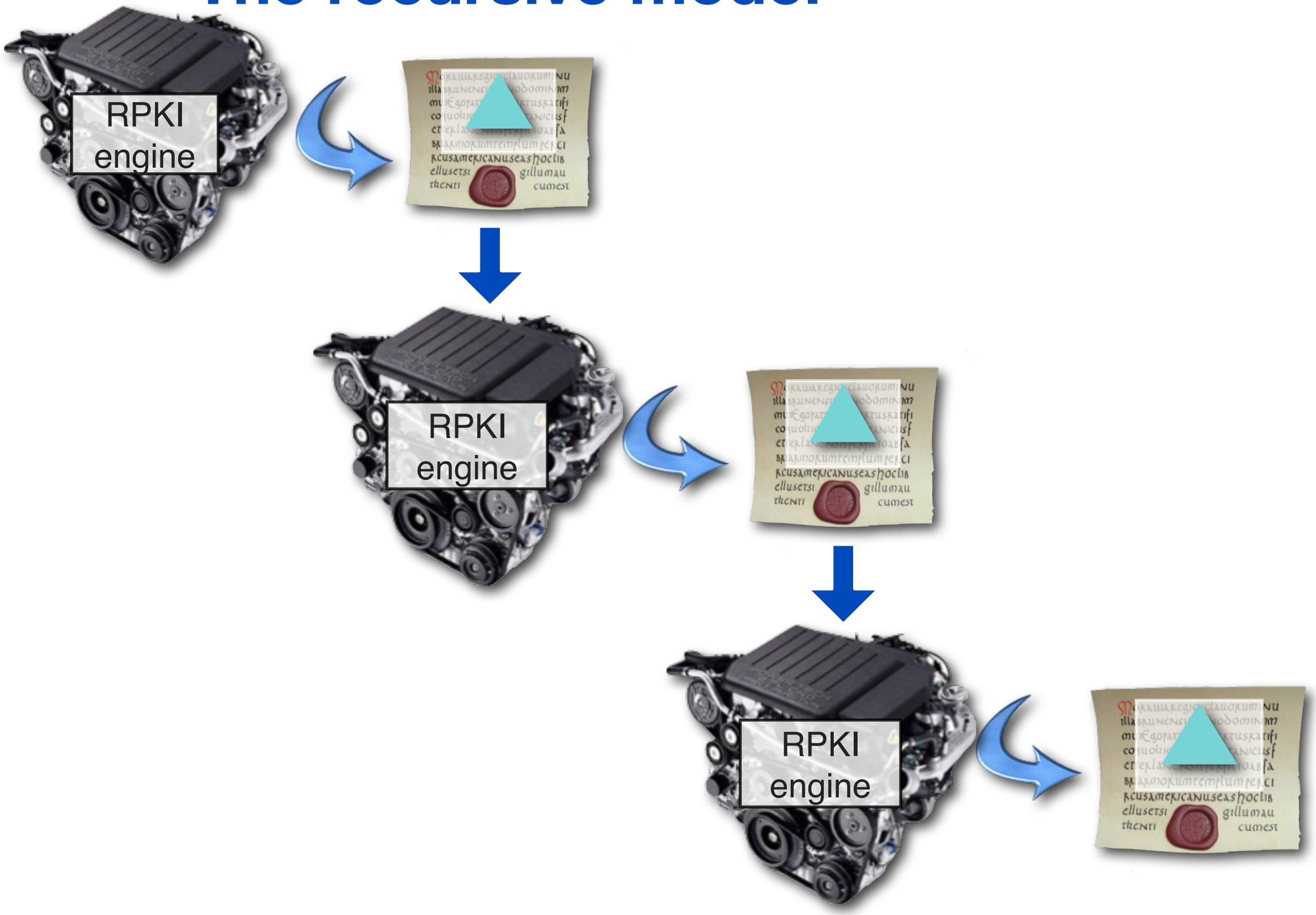
Added value

- Certificates can be the inter-regional exchange standard between RIR's
- Facilitates automated provisioning
  - easier to prove holdership than through "detective work"
  - certified information in parseable format
- (Long term) Could help future secure routing
  - fills need for a PKI infrastructure and trusted third party
- Support resource (IPv4, IPv6, ASN) transfers

The RPKI engine generates certificates for a lower level



The recursive model



The wider picture

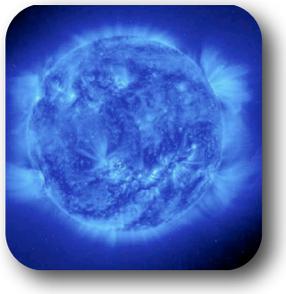
- Our (development team's) primary goal may be getting certification implemented...
- But we can't do this in a vacuum!
  - How does policy affect certification?
  - How does certification affect RIPE NCC's processes?
  - Where does certification fit in the processes?
- There is a strong interdependence between technical implementation, processes and policy

Please follow related discussions in Address Policy and Routing working groups as well

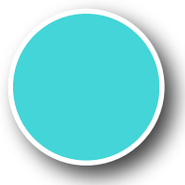
Even more tangible...

Scenario

Please
route this network
for me



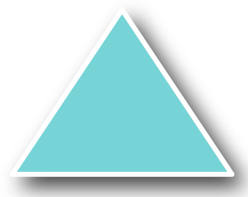
BlueLight ISP



AS65000

Hmm, is MiniCorp
really the holder of that
resource?

MiniCorp



10.0.0/21

Automated Provisioning

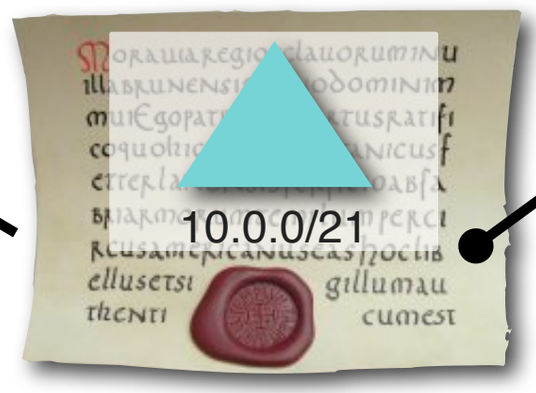
- Provisioning an IP Resource
  - Does Holder **really** hold the resource?
- Checking takes detective work
  - Takes manpower
  - Needs specific knowledge and skills
- Is there an easy and secure way?
  - Meet the Route Origination Authorization (ROA)

Meet the ROA

- Secure: only true holder can create
- One-sided: states permission of address space holder only
- Multiple ROAs for one prefix allowed

Relation ROA — Resource Certificate

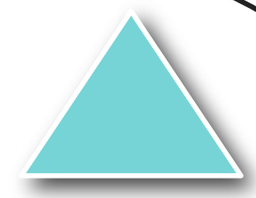
MiniCorp's
resource certificate



One-time certificate
(EE certificate)

Scenario: conversation

Please route this network for me

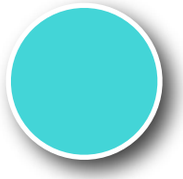


10.0.0/21

MiniCorp

BlueLight ISP

Hmm, is MiniCorp **really the holder of that** resource?

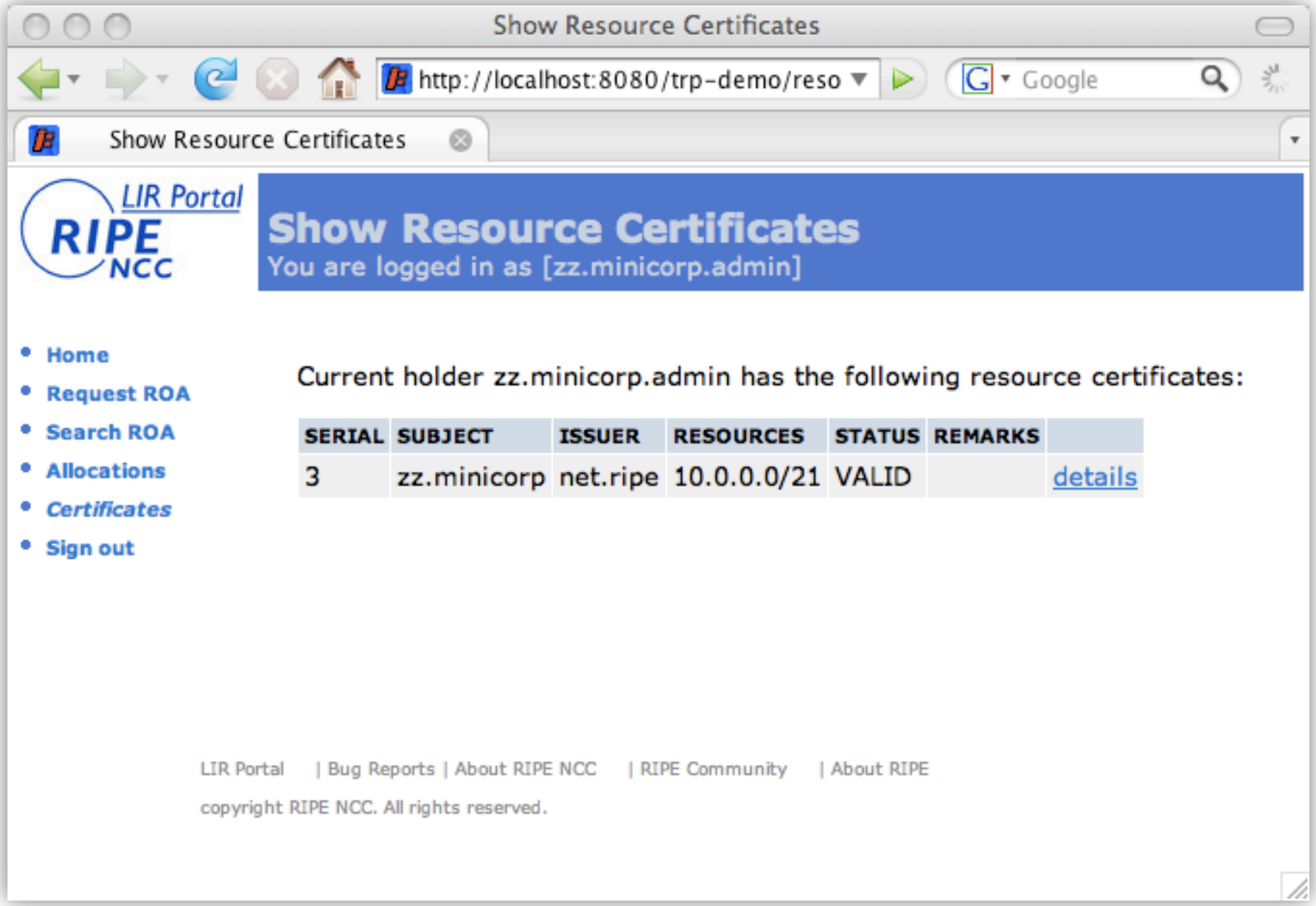


AS65000

Okay, please **sign a ROA** with my ASN

Demo Automated Provisioning

Join certification test program



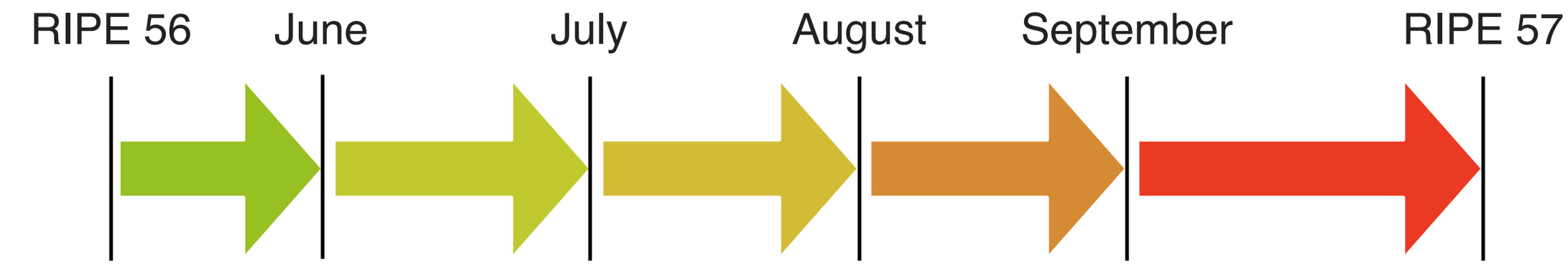
Join certification test program

- What is there for you:
  - sneak preview of certification implementation (web interface)
  - your input taken into account in further development
  - help to get started (documentation, screencast...)
  - mailinglist to share experience: certtest@ripe.net
- What is expected from you:
  - send participation request to certtest-request@ripe.net
  - be prepared to spend 1–2 hours for testing functionality every month
  - give us feedback
- period: May – September

Functionality outlook

- Certificates for your PA allocations
- Certificate/key management (revocation, key rollover)
- ROAs
- Transfer support
- Recursive model (hosted/not hosted)

Timeline


RIPE 56
June
July
August
September
RIPE 57
Production-ready release
Functional update
Functional update
Functional update
Enable
member test

The team

Andrew de la Haye
COO – driving project

Trudy Prins
project manager

Oleg Muravskiy
software architect

Questions?