Developing a Routing PKI
or
Certification of Internet Resources

Henk Uijterwaal
RIPE NCC
UKNOF-8, September 2007

Agenda

- Why are we doing this?
- Efforts in this area
- RIPE NCC efforts
- How you can contribute?
- Conclusions and questions

Why are we doing this?

- New trends emerging:
- Trading of IPv4 resources
- Address and routing security

Trading of IPv4 resources

- Sooner or later, we'll run out of IPv4 addresses
  - RIRs will have to say no to requests for new addresses
  - May 2010?
  - Not every network will be IPv6 ready by then
  - There will still be a demand for IPv4
- Solution: See if one can get IPv4 from others
  - Some no longer need their IPv4 addresses
  - Buy or borrow, but don't steal
- A market for IPv4 will emerge

Trading of IPv4 resources

- Issues in a market:
  - Is the person offering me the resource authorized to do this?
  - How do I know that I'm the only buyer?
  - How do I show that I'm now authorized to use the resource?
- Similar situations (house, car, …): Certificate of ownership
- This could be done for addresses as well

Address and routing security

- Basic security questions
  - Is this a valid prefix?
  - Who injected it into the network?
  - Is the person who did this authorized to do this?
  - Is the forwarding path acceptable?
  - Can I trust my peer to deliver accurate information?
- Answers have to be
  - Reliable
  - Fast
  - Cheap

Address and routing security

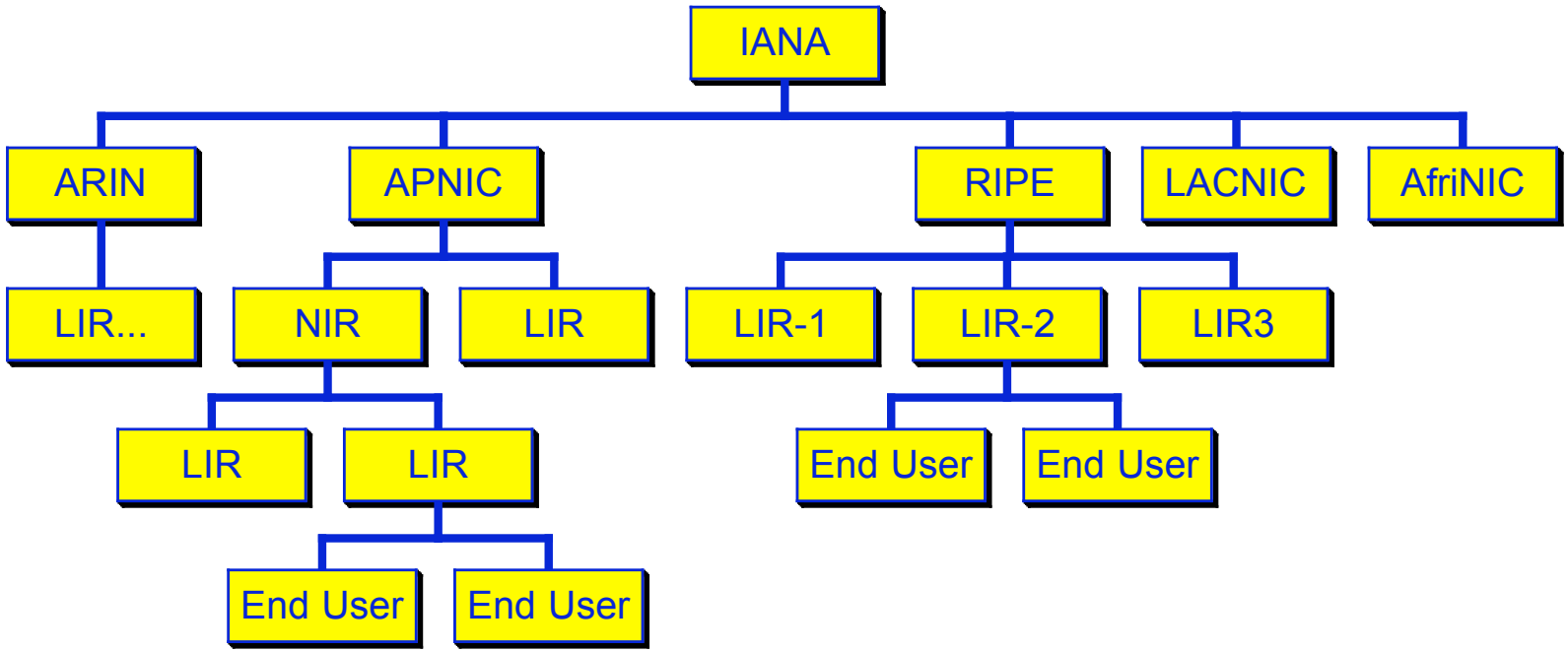
- Potential technologies
  - *Improved* Internet Routing Registries
  - DNS/DNSSEC
  - Signed peerings
  - Certificates
  - …
- Certificates can be used for both trading and address security
  - What is a certificate?

Public Key Infrastructure

- Public/Private key pairs can be used to sign and encrypt messages
  - Sign with private key, Check with public key
  - Valid signature: the message originated from the owner of the private key and has not been tampered with
  - But these are just series of bits…
- Public Key Infrastructure deals with:
  - Who issued these bits?
  - When are they valid?
  - Where/how can they be used?

PKI

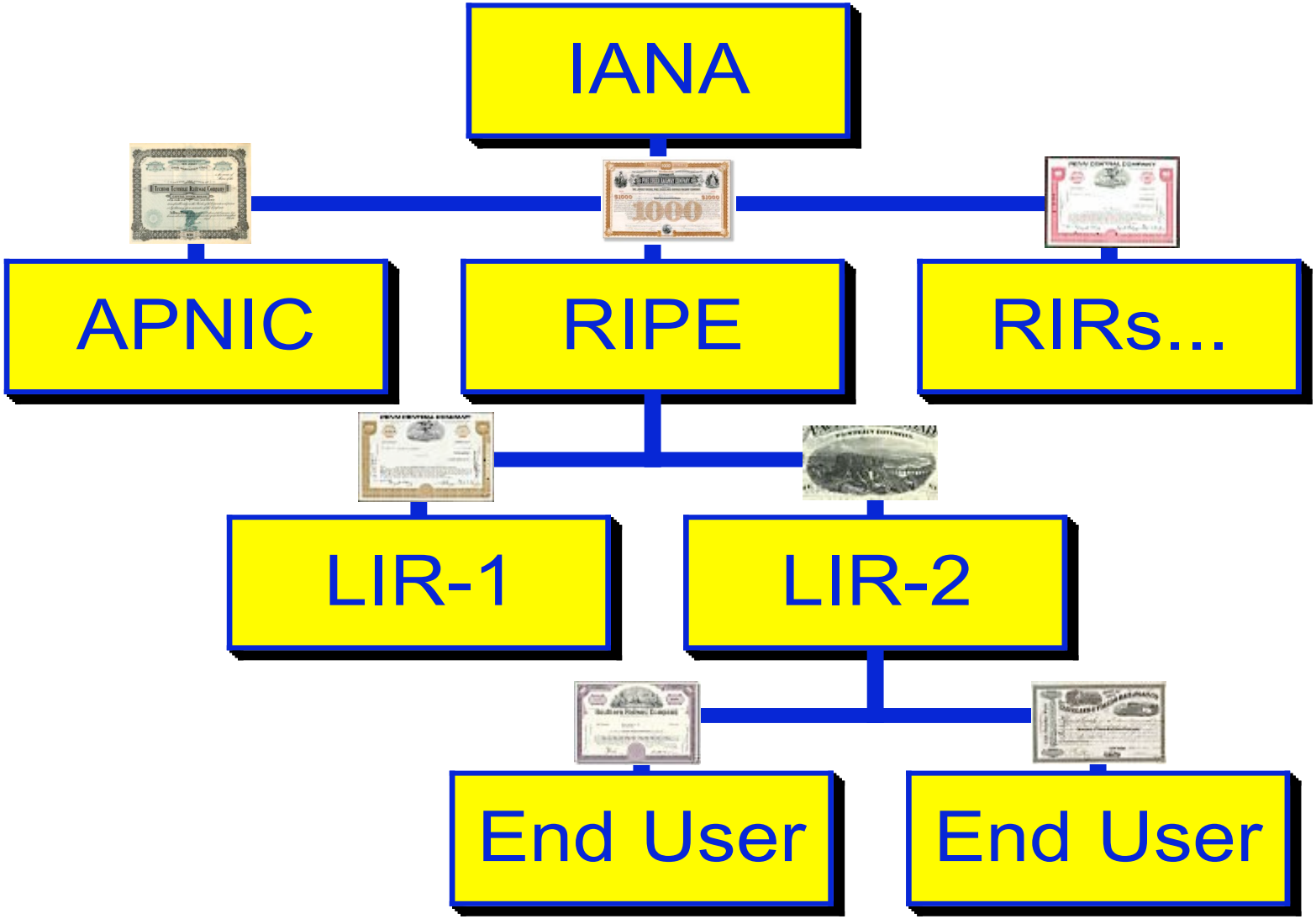
- Various ways to set this up
- Hierachy seems best suited for this case
- Mirrors address allocation hierachy



Certificates

- What is a certificate?
  - Structured file with information
  - Signed with a private key
  - X.509 is the standard
- Properties
  - Valid for a certain period
  - Can be revoked
  - Allows for generating subordinate certficates
  - Validity can be checked by walking backwards to the root

The full tree...



Let's set this up for resources…

- Not that simple:
  - More than technology
  - Also organizational, procedural and legal aspects
- Issuing certificates
  - Identification of the parties
  - Validation
  - Revocation
  - Allocation of blocks downstream
  - 2 purposes:
    - Authorized user
    - ROA

Let's set this up for resources… (2)

- Practical: 10,000 LIRs world wide, with 100,000's of customers
- Other requirements
  - Use existing standards and technologies when possible
  - Extend function of existing organizations, no new organizations
  - Should fit into the existing frameworks
  - Incremental deployment
  - Reliable, trustable and efficient results
  - Don't force anybody to make authoritative claims beyond its actual knowledge

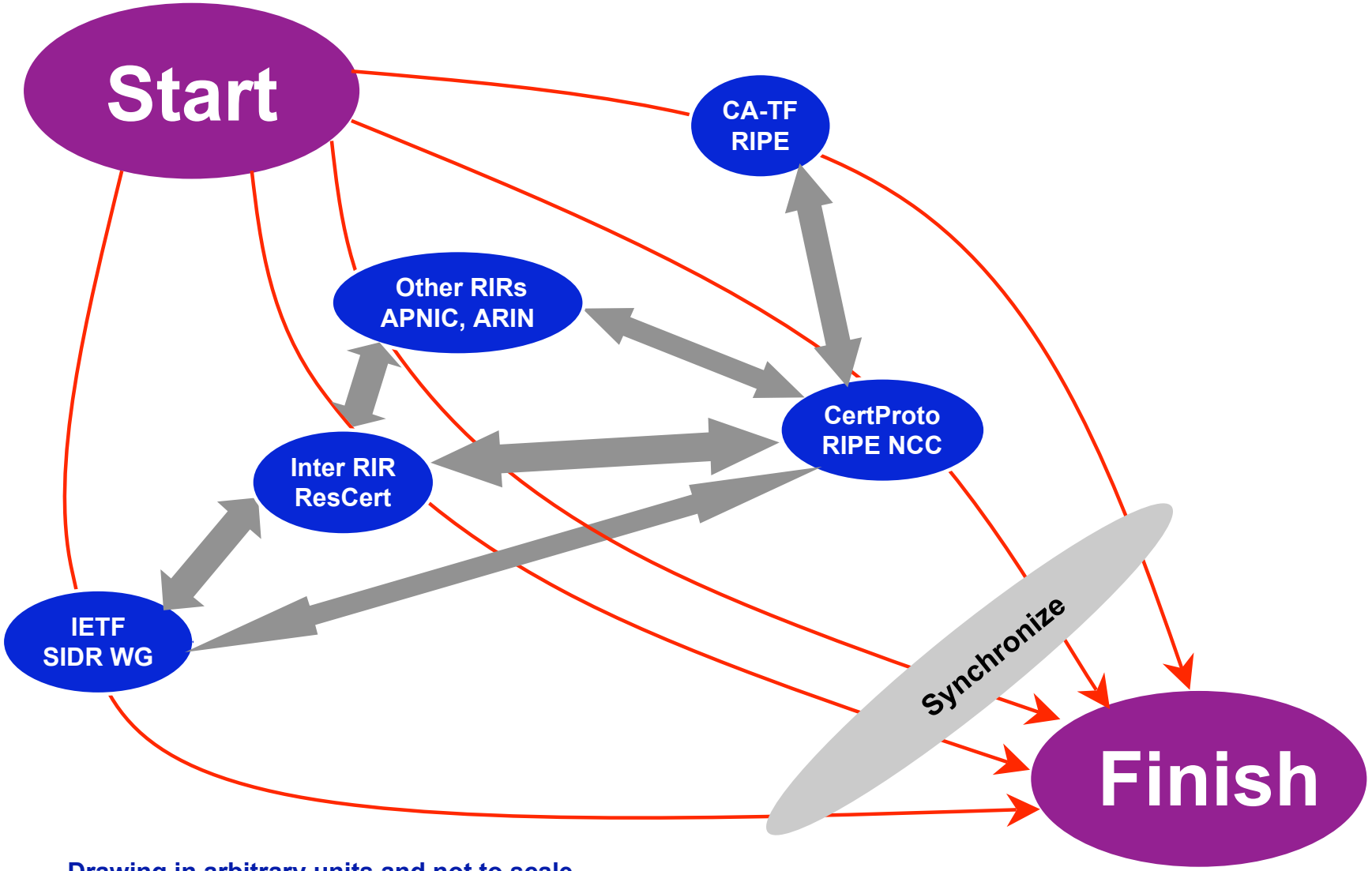
Do we have to do this?

- Not certain, but use cases are very likely to occur
  - IPv4 will run out, something will have to happen then
  - Routing security is become more and more important
    - Government pressure
- Long time to develop this
  - Can’t wait until people actually ask for this

Efforts in this area

- SIDR-WG/IETF
  - Working group to formulate a standard architecture for a secure inter-domain routing security framework
- ResCert/Inter-RIR coordination
  - Provide a common system across RIRs, discuss common issues amongst RIRs
- RIPE/CA-TF
  - Provide guidance to the RIPE NCC from an LIRs view
- RIPE NCC/CertProto, CertDeploy
  - Evaluate the consequences for the NCC operations and systems
  - More on this project later
- Activities at ARIN and APNIC

Relation between these efforts

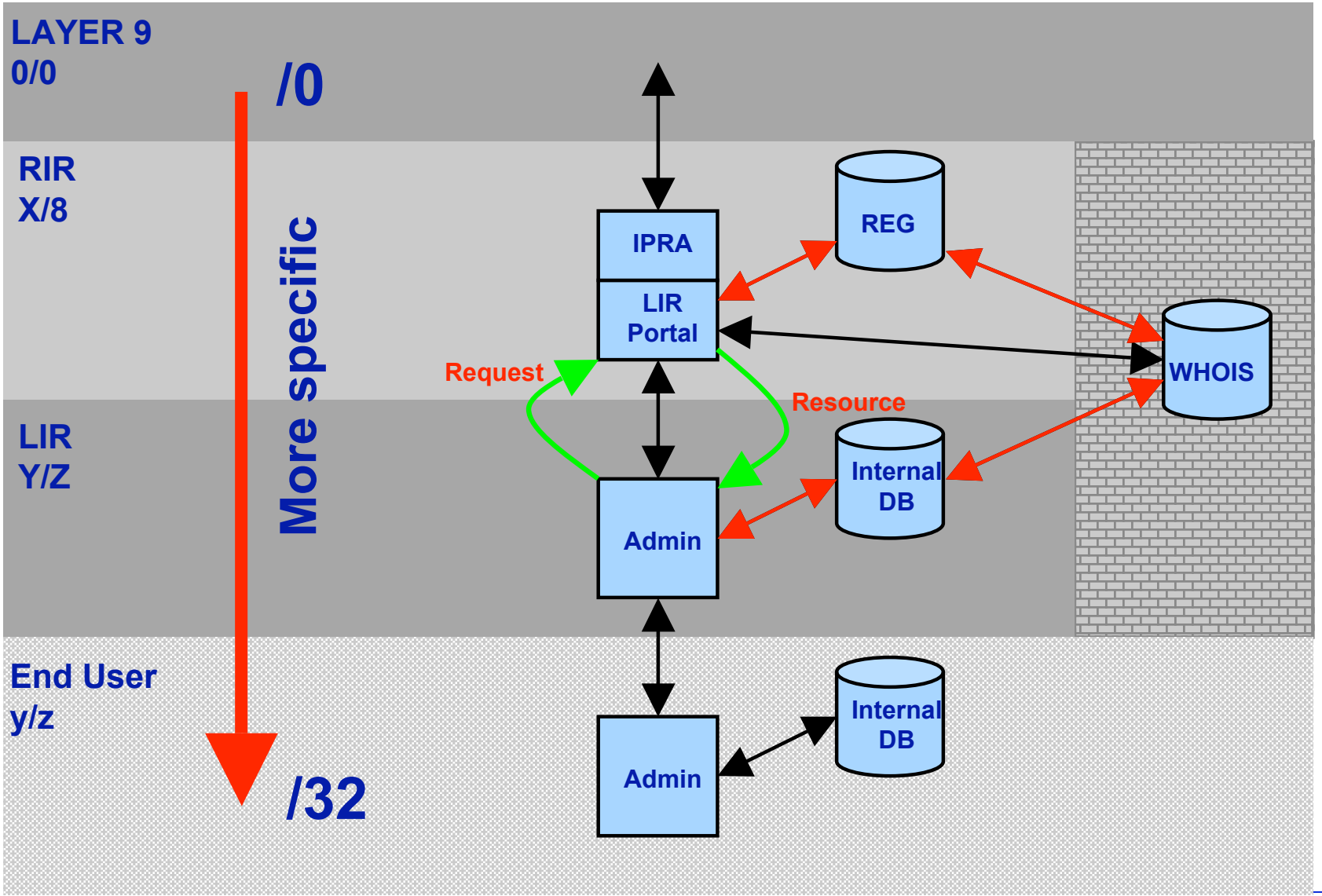


Drawing in arbitrary units and not to scale

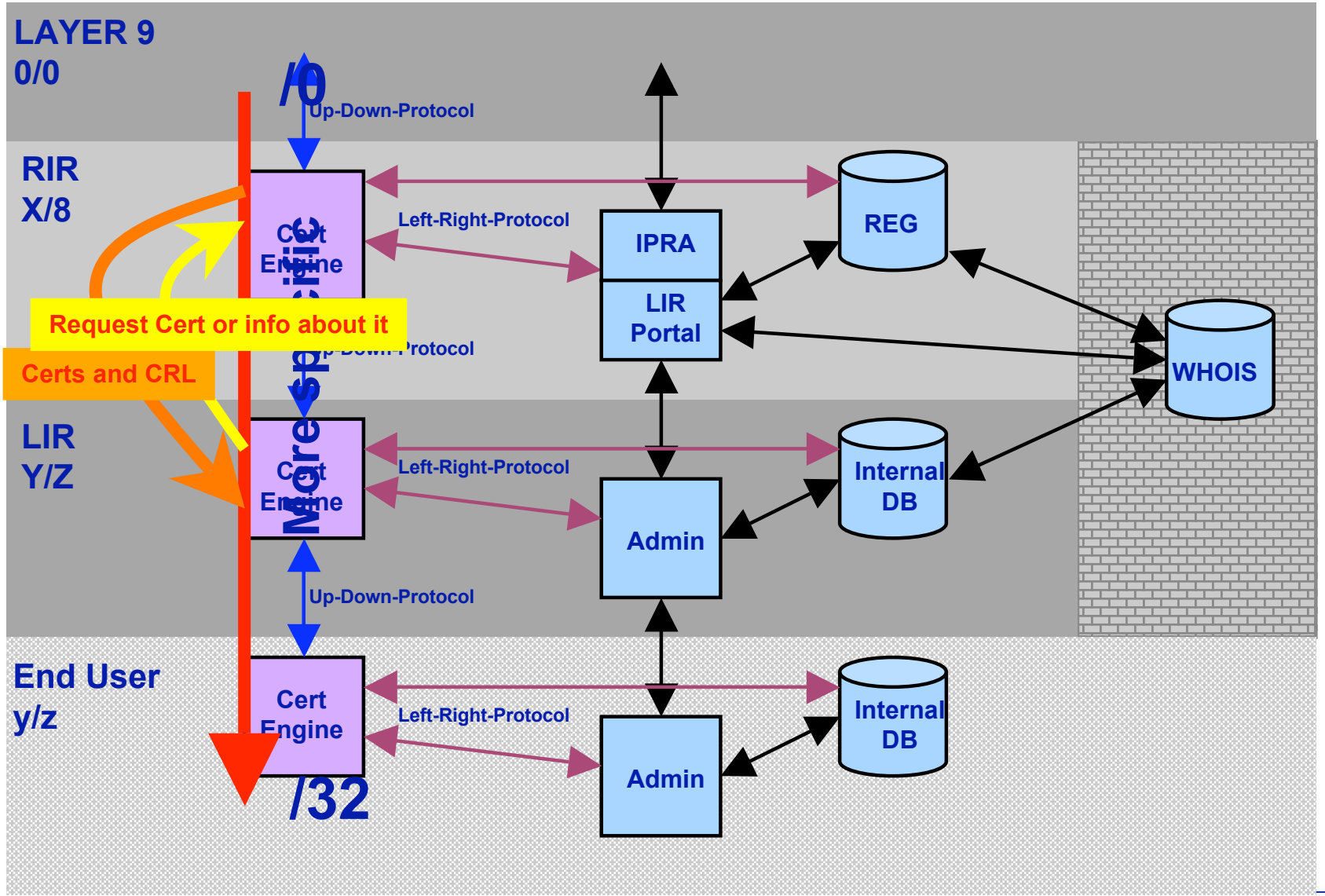
Current view of the system

- System to hand out certificates
  - X.509 with IP/AS extensions (RFC 3779)
  - System runs in parallel with existing procedures
- Functional layout
  - Extensive discussions between all parties
  - Rough consensus
  - Different implementations of elements are possible, but common interfaces
  - Details still being discussed but converging

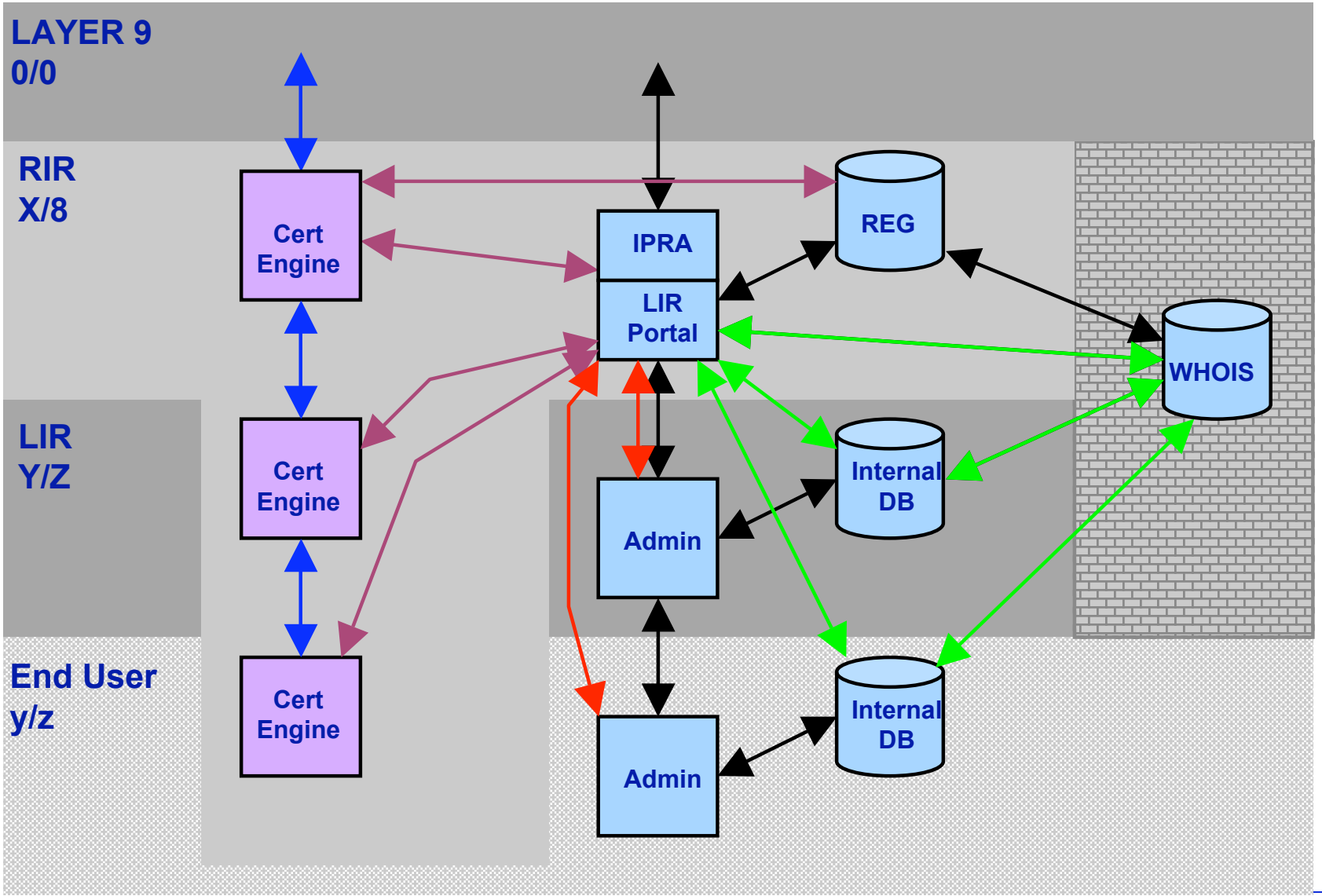
Current situation



The future


LAYER 9
0/0
/0
Up-Down-Protocol
RIR
X/8
Cert Engine
Left-Right-Protocol
IPRA
LIR Portal
REG
WHOIS
Request Cert or info about it
Certs and CRL
More specific
LIR
Y/Z
Cert Engine
Left-Right-Protocol
Admin
Internal DB
Up-Down-Protocol
End User
y/z
Cert Engine
Left-Right-Protocol
Admin
Internal DB
/32

Outsourced CA (aka hosted CA)



What has the RIPE NCC been doing?

- 2004-2005: “This might be of interest for us”
  - Read up
  - Attend workshops/BOFs, followed mailing lists
- 2006: “Getting serious”
  - 1.2 FTE as of 1/3/2006
  - Initial studies
  - Understand technology
  - Introduce this to RIPE community:
    - CA Task Force for community input
- 2007:
  - CertProto Project: January-August 2007
  - CertDeploy Project: September 2007-??

CertProto Project

- External Goal: Enable CA-TF to do their work
- Internal
  - Goal: Understand all aspects of building and integrating a certification system for Internet resources before we actually start building it
  - Objectives:
    - Build a prototype (1/3/2007)
    - Report at RIPE 54 (May 2007)
    - Full report for management review (June 2007)
    - Plan forward (summer 2007)

People on the team

- BA: Tim Bruijnzeels, Trudy Prins
- COMMS: Chris Buckridge
- DB: Denis Walker
- FIN: Sonia Garbi Gomez
- POL: Filiz Yilmaz
- RS: Xavier Le Bris , Alex le Heux, Mike Petrusha,
- SG: Robert Kisteleki, Rene Wilhelm
- CA-TF liaison: Andrew de la Haye

- PM: Henk Uijterwaal

Work Areas

- Support for CA-TF
- Prototype
- Business Analysis/System Analysis
- Data Accuracy
- Financial aspects
- Policy

Prototype

- Why?
  - Certification: X.509 well tested but application to Internet resources is new
  - Little experience at the the RIPE NCC
- Built and delivered a prototype
- Based on assumptions
  - Correct at the time we designed it, but things have evolved since then
  - Standards were not defined
  - Business analysis not done

Prototype (2)

- Delivered 1/3/2007
- Successful testing internally
- Conclusion:
  - Approach works but too much hands on work for all partners
  - Fed conclusions back into design shown earlier
  - Tossed the prototype away

Business analysis & Systems analysis

- BA: Looked at current operations and added certification to it
  - Identified processes that need modification
  - Identified processes that we need but don't have
  - Modeled all processes with UML
- SA: How does this affect our systems?
  - Main component: REG, our authoritative, internal DB
  - Will need a lot of modifications…
  - … but there is a project to re-write it anyway
  - Our requirements are known and included

BA example: Issue Certificate

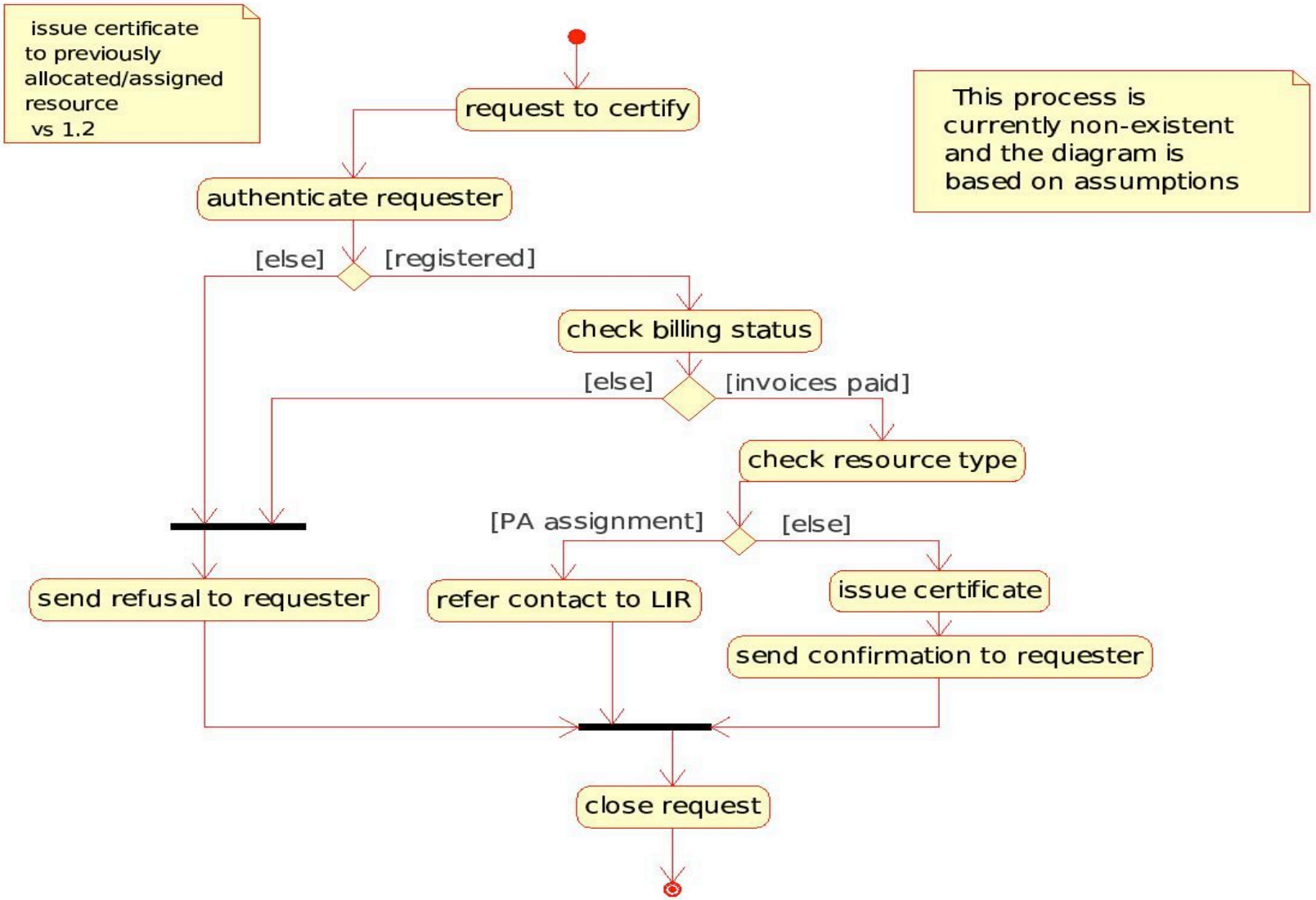


Diagram: issue certificate current resource Page 1

Business analysis & System analysis (2)

- Conclusion:
  - Verified that our processes and the current view of the system are compatible
  - Identified which modifications are needed
  - Listed all issues that need to be resolved (and aren't show-stoppers)

- This will be translated into detailed requirements for the final system

Data accuracy

- The system will use registration data from the Internal DB and the RIPE DB
  - Problems if the data is inconsistent
- Checked this: **≈99%** of the data is internally consistent
  - Quite good
  - Defined specific actions to improve
- Not a problem
  - Note: This does not deal with DB versus Real life

Financial and policy aspects

- What will happen to your membership fees if we introduce this service?
  - Issues:
    - Development
    - Maintenance
    - Various scenarios
  - Effects at the few % level
- Do we have to change existing policies?
  - Yes, identified
  - Proposals will come later

CertDeploy Project

- Towards an actual certification service offered by the RIPE NCC to its members
- Deliverables:
  - Produce a system that supports all operations needed by a future RIPE NCC certification service
    - Hardware
    - Software
    - Documentation (both technical and user)
    - Draft CP and CPS documents for the RIPE community
  - Produce components that can be used by the community to build tools for operations themselves and/or be able to use our service (ie. RPKI Engine + Back End stub)
  - Draft proposals for policy modification to be put in the PDP

CertDeploy/Objectives

- Inform community on the development:
  - RIPE meetings
  - Regional meetings/user groups
  - CA-TF meetings
- Collaborate with ResCert team and other RIRs
  - Interfaces and inter-operability
  - Consistent plans
- Work in a way that is flexible enough to adapt to changing external constraints
- Ensure sufficient quality of all S/W for a production situation
- Gain understanding about the implications of providing a certification service by the departments that will be involved in service delivery.

CertDeploy/Non goals:

- No decision yet if this service will be offered by the RIPE NCC
  - Don’t introduce this as production service to our members
  - No detailed roll-out plan
  - Don’t develop SLAs/SCMs
  - Don’t develop user training for the LIR course

Planning

- Lots of work:
  - 6-9 months of work
  - Start October
  - ≈ 5 FTE
- Currently being scheduled

Pointers and URLs

- SIDR WG
  - http://www.ietf.org/html.charters/sidr-charter.html
  - 6 architecture documents
  - Read and comment!
- RESCERT:
  - http://mirin.apnic.net/resourcecerts/wiki/index.php
  - Information repository
- CA-TF
  - http://www.ripe.net/ripe/tf/certification
  - Public website of closed group
- CertDeploy: will have a website…

Conclusions

- New trends in the industry may require certification of resources
- RIRs have to be ready to issue these certificates
- RIPE NCC well on its way to have this service

Questions?