Developing a Routing PKI
or
Certification of Internet Resources

Henk Uijterwaal
RIPE NCC
MENOG II - November 2007

Agenda

- New Trends Emerging
  - Trading of IPv4 resources
  - Address and Routing Security
  - Certification of resources
- What is a certificate?
  - 10 minute overview of the technology
- Deployment by the RIRs

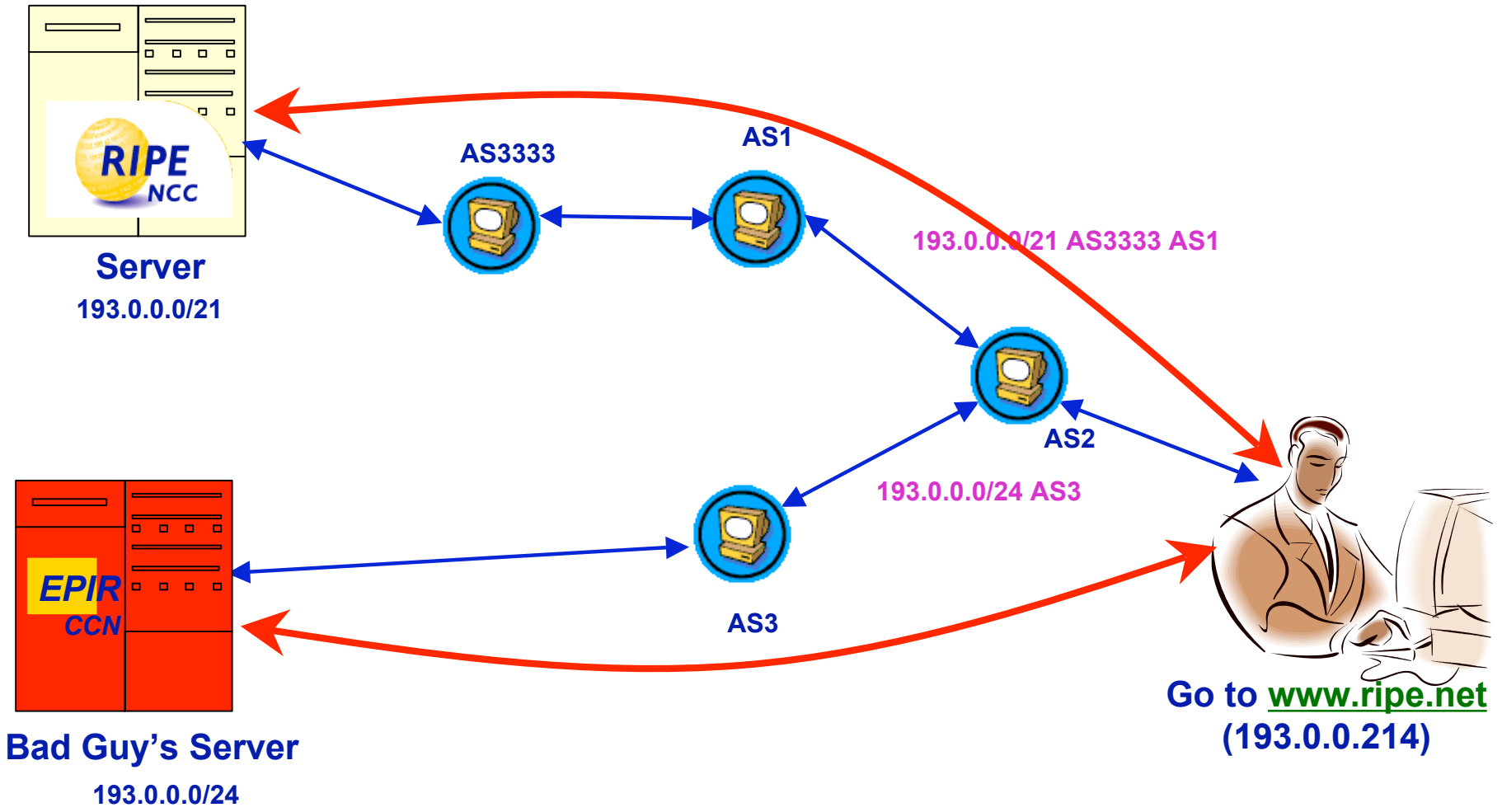
Trading of IPv4 resources

- Sooner or later, we'll run out of IPv4 addresses
  - August 2010? June 2011? …
  - Not every network will be IPv6 ready on that day
  - 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

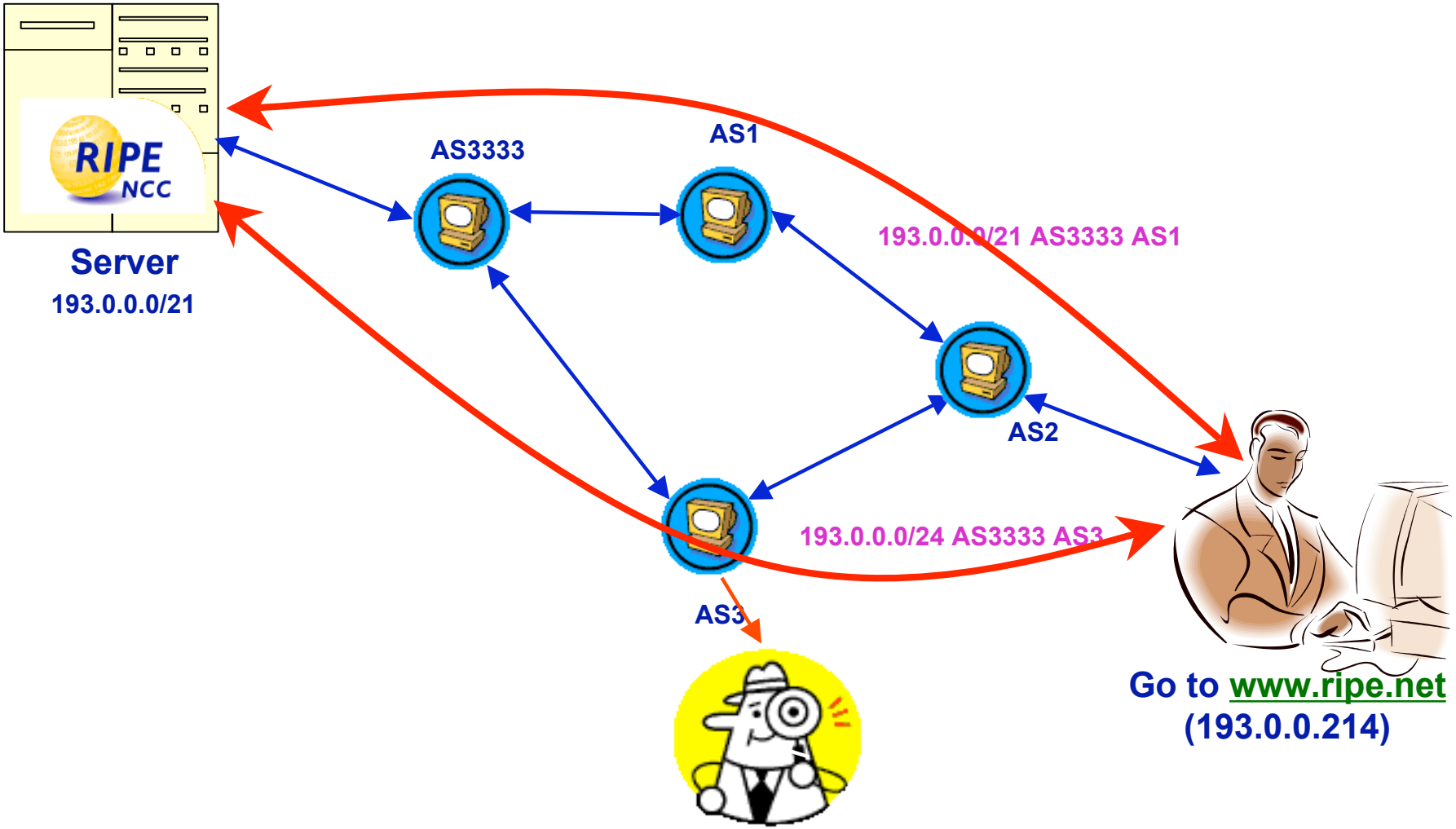
Trading of IPv4 resources

- 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: *Certificate of ownership*
  - House, Car
- This can be done for addresses as well

Address and Routing Security



Address and Routing Security (2)



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?
  - How does this work?

What is a certificate?

- A document issued by a well-known authority that says that the holder is allowed to use something

- In this case:
  - Structured computer file (X.509)
  - Contains information about the addresses
    - Range (IPv4, IPv6, ASN)
    - Who assigned this
    - Validity dates (“good through…”)
  - Digitally signed using Public Key Technology

Public Key Technology

- A technique to sign and encrypt messages
  - Uses some really weird mathematics
- Two independent keys:
  - Publish one key: “Public key”
  - Keep the other secret: “Private Key”
- Use:
  - Private key to *encrypt* messages
  - Public key to *decrypt* messages

Public Key Technology

- "Hello, I am Henk"
- 25b2d2325bab59804fb8083e
- "Hello, I am Henk"

- Original message
- Encrypted with private key
- Decrypted with public key

Message must be from owner of the private key

- 25b2d2325bab59804fb8083f
- "XyZR%@r12rwe"

- Modify the message…
- Can't decrypt

Message cannot be modified during transport

- "Hello, I am Hank"
- 2347dc609af964c9e28086ce

- Guess message
- You can't

Cannot generate message without private key

More properties of certificates

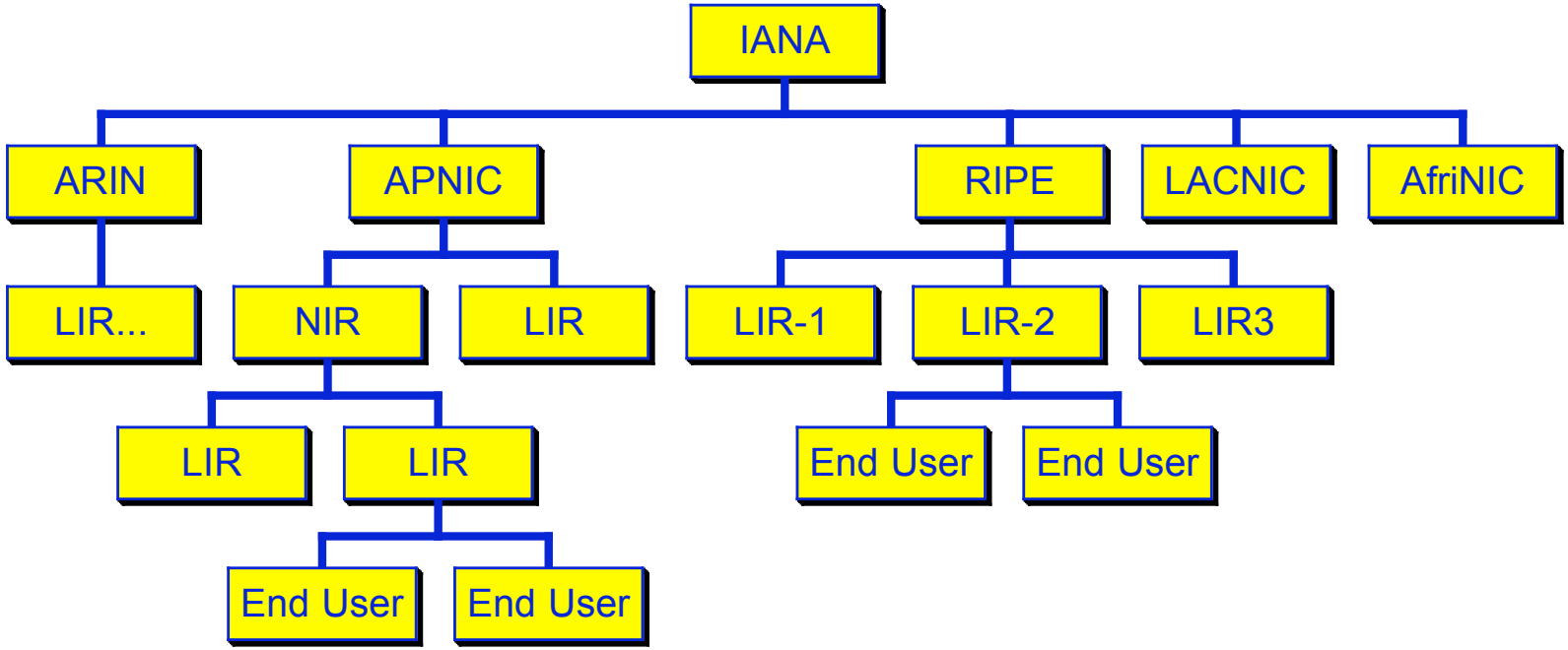
- Valid for a certain period
  - "RIPE NCC can use 193.0.0.0/21 from 1/1/2007 to 31/12/2007"
  - Expires afterwards
  - Can be revoked earlier
- Allows for generating subordinate certificates
  - "RIPE NCC's RIS project can use 193.0.1.0/24"
  - Issued in a tree-like fashion
  - Validity can be checked by walking backwards through the tree

Public Key Infrastructure (PKI)

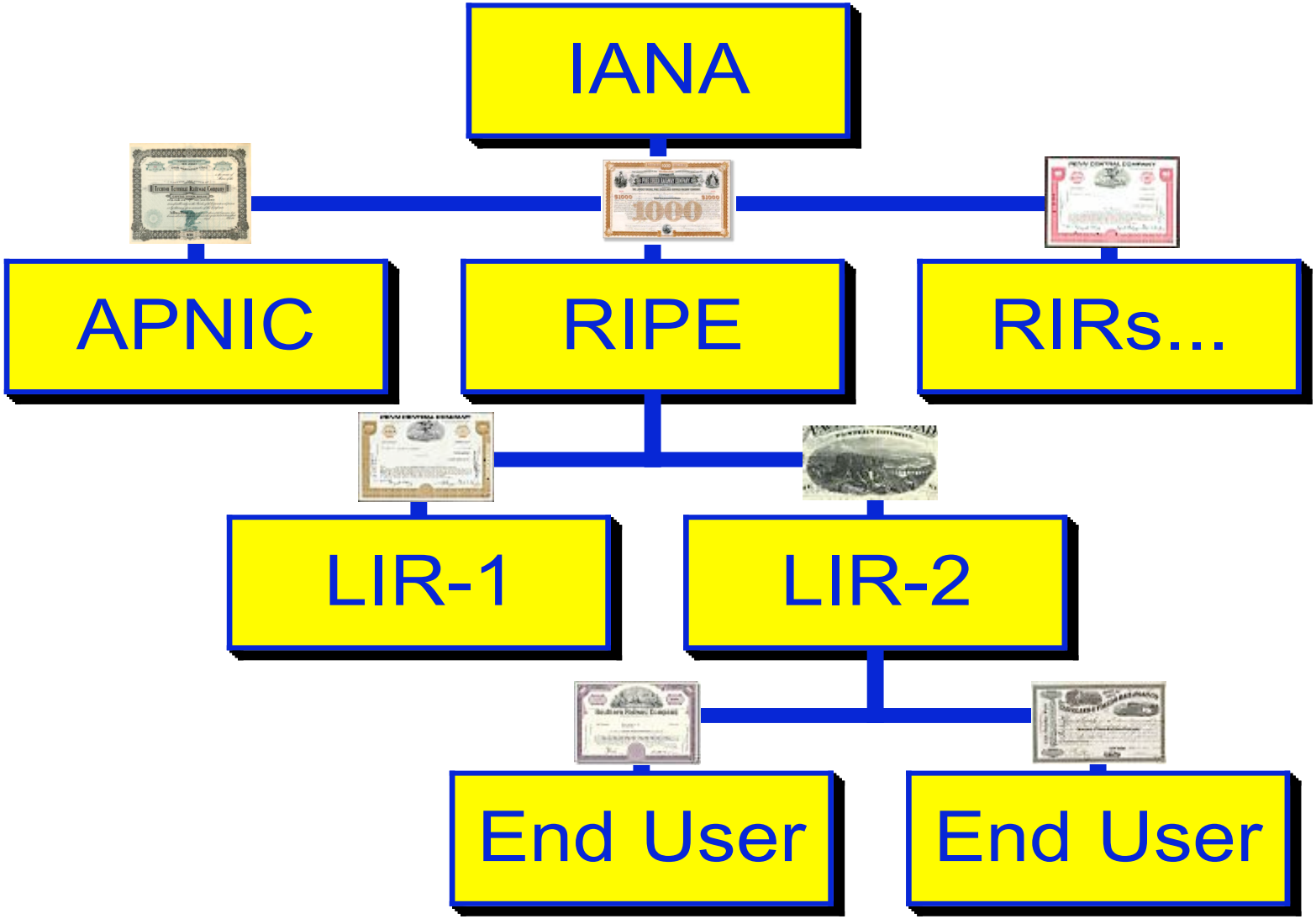
- Key pairs are series of bits
- Public Key Infrastructure deals with:
  - Who issued these bits?
  - When are they valid?
  - Where/how can they be used?

PKI

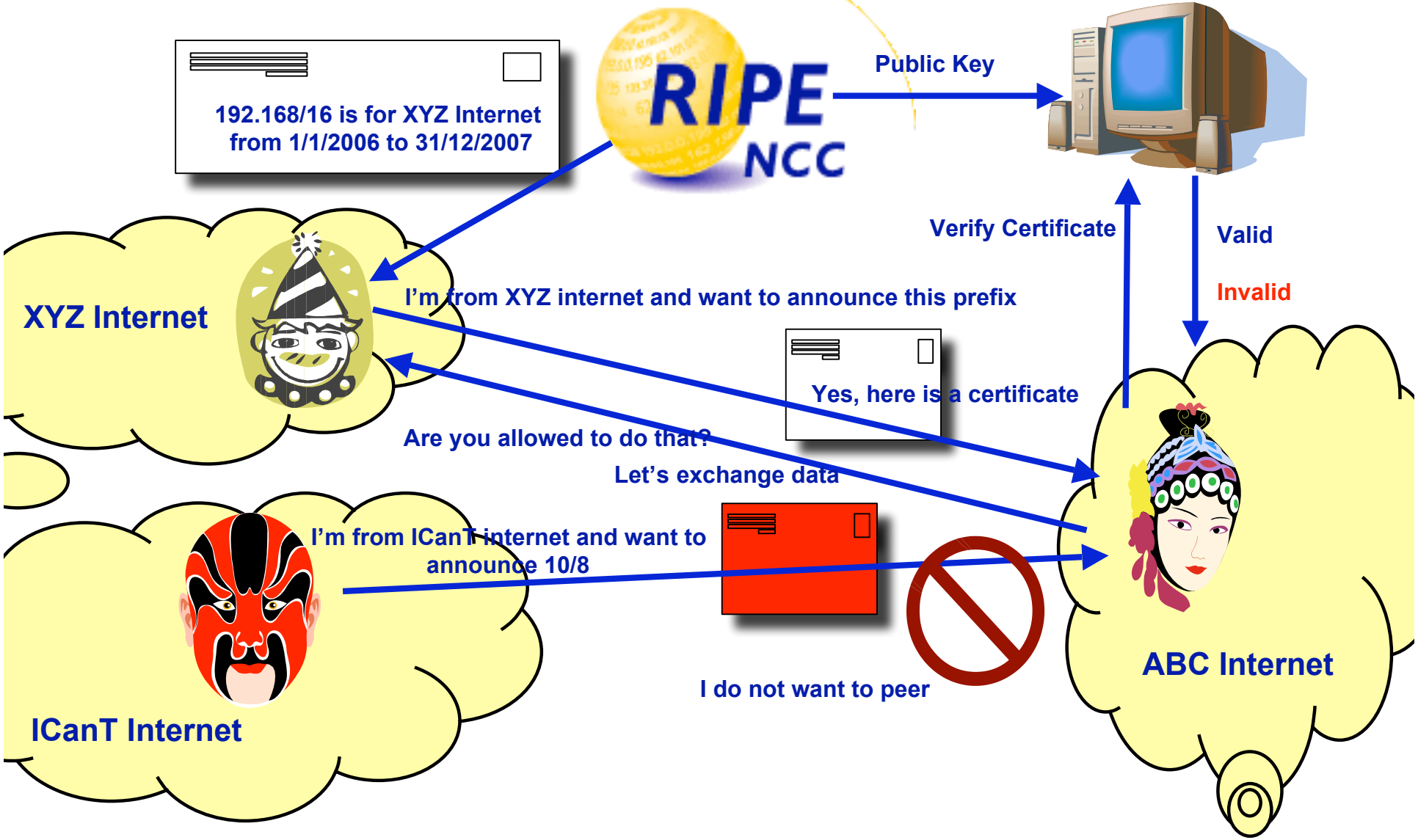
- Various ways to set this up
  - Hierachy seems best suited for this case
  - Mirrors address allocation hierachy



The full tree...



Putting it all together



Let's set this up…

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

Let's set this up… (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

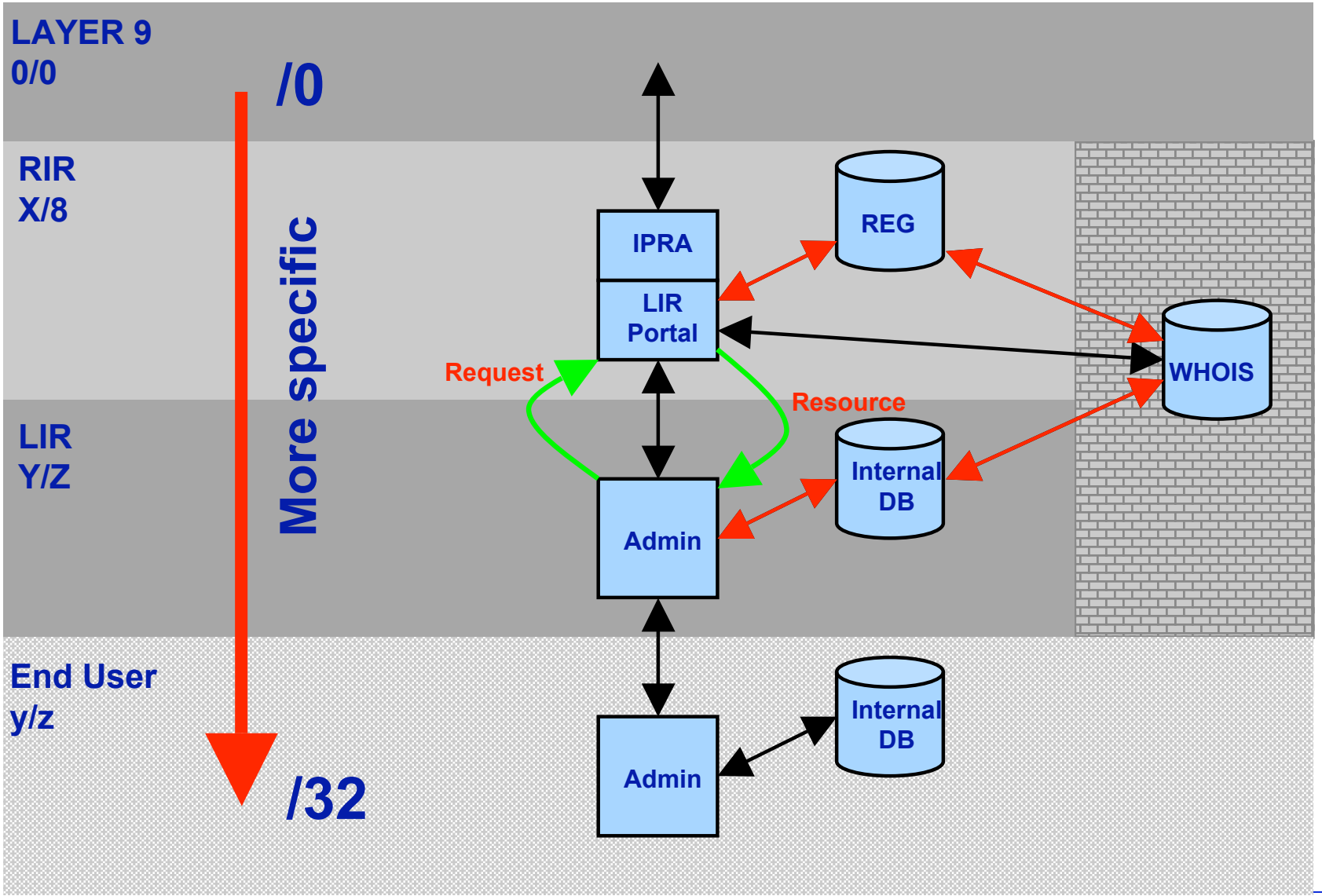
Do we have to do this?

- 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

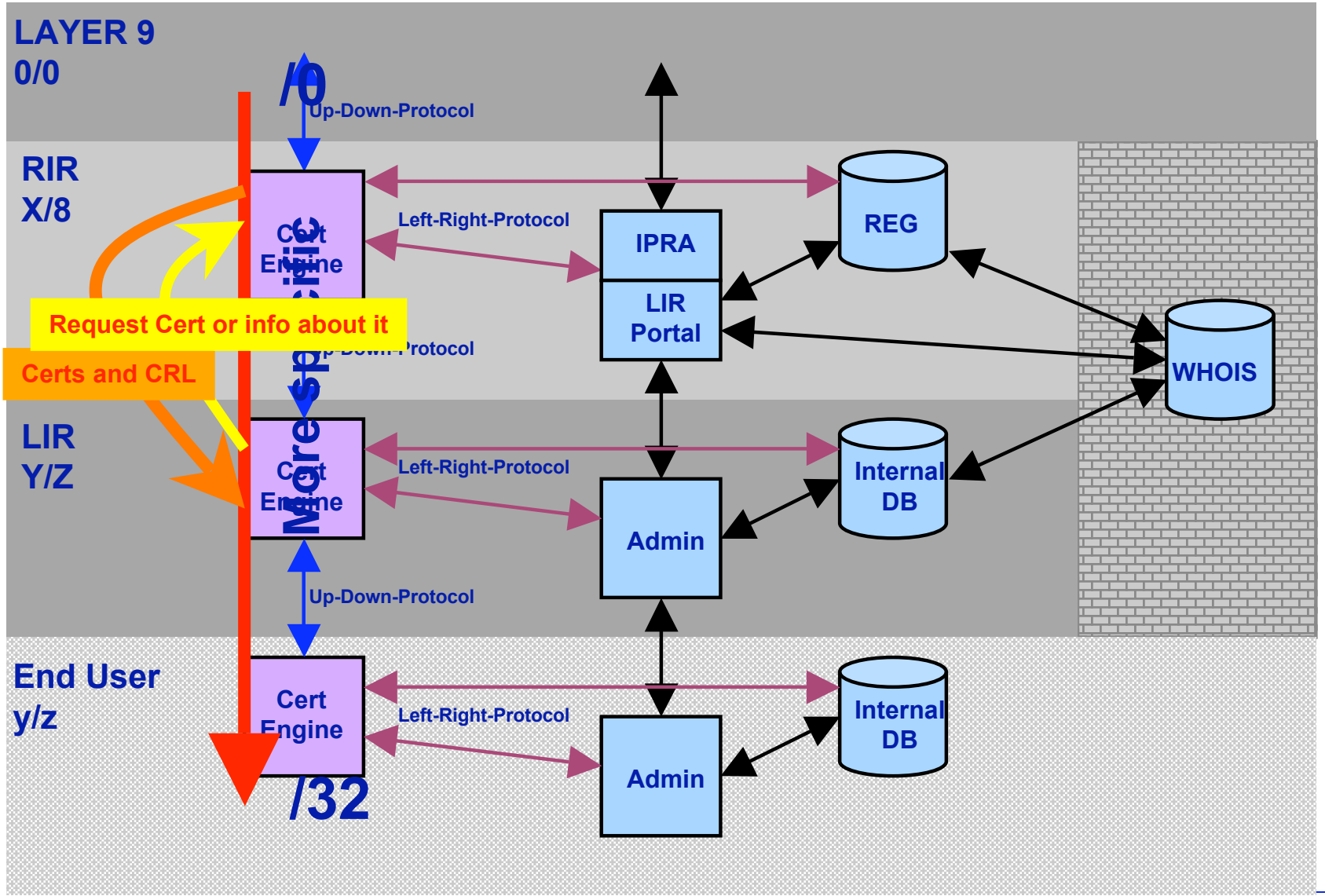
Current view of the system

- 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

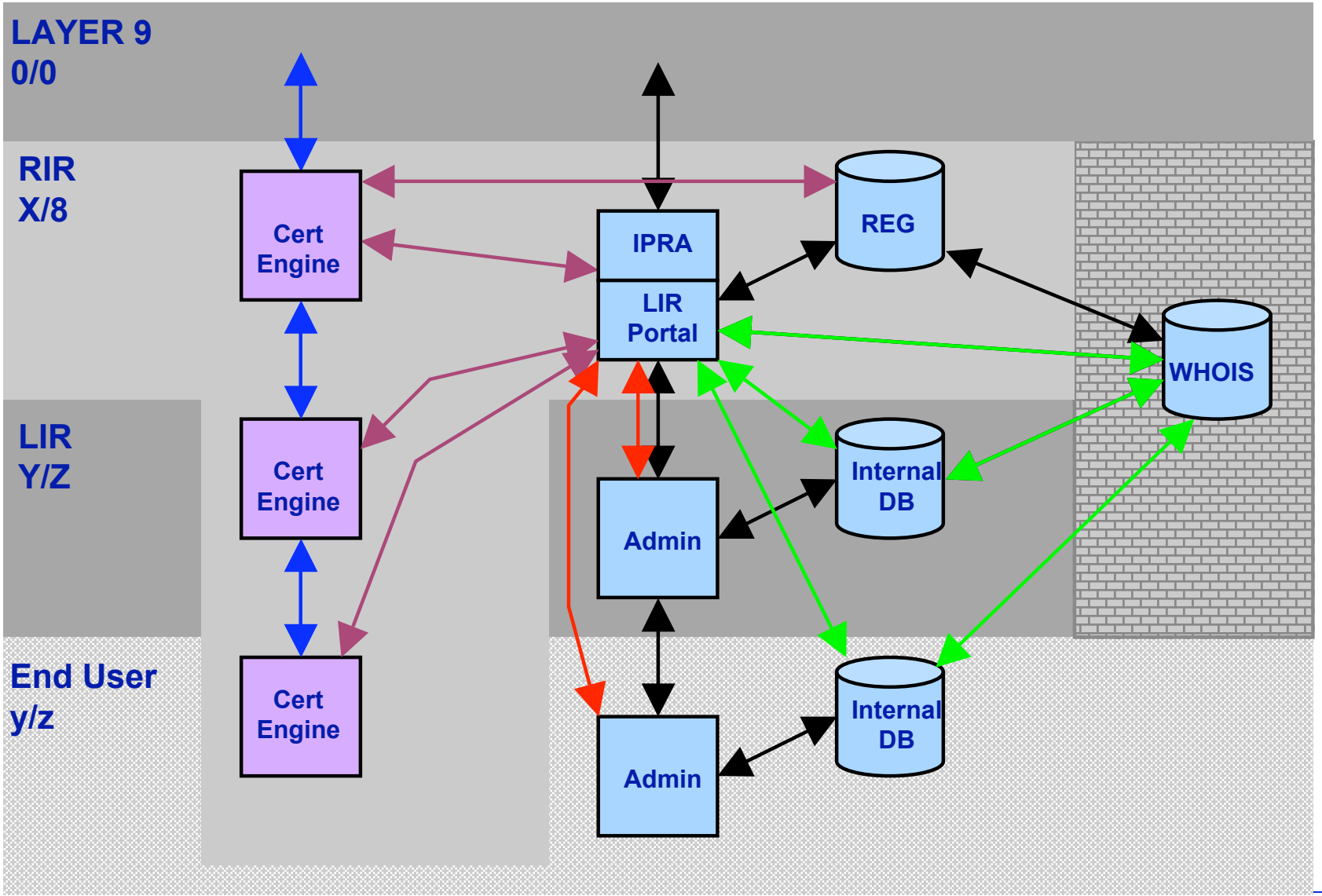
Current situation



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: “Build something”
  - CertProto Project: January-August 2007
  - CertDeploy Project: October 2007- May 2008

CertProto Project

- Goal: Understand all aspects of building and integrating a certification system for Internet resources before we actually start building it
- Fall 2006 - Spring 2007
- Successfully completed

CertDeploy Project

- Towards and actual certification service offered to the RIPE NCC members
- In parallel with efforts at other RIRs
- Now - Spring 2008

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
- Technology to do this is being developed