



CertProto

Understanding the consequences of introducing certification at the RIPE NCC

Henk Uijterwaal

RIPE 54

9 May 2007



Introduction

- **Background**
- Current view of the certification system
- RIPE NCC CertProto Project
- Conclusions



Overall Goal

- Introduce certification of Internet resources
 - Motivation in TF slides

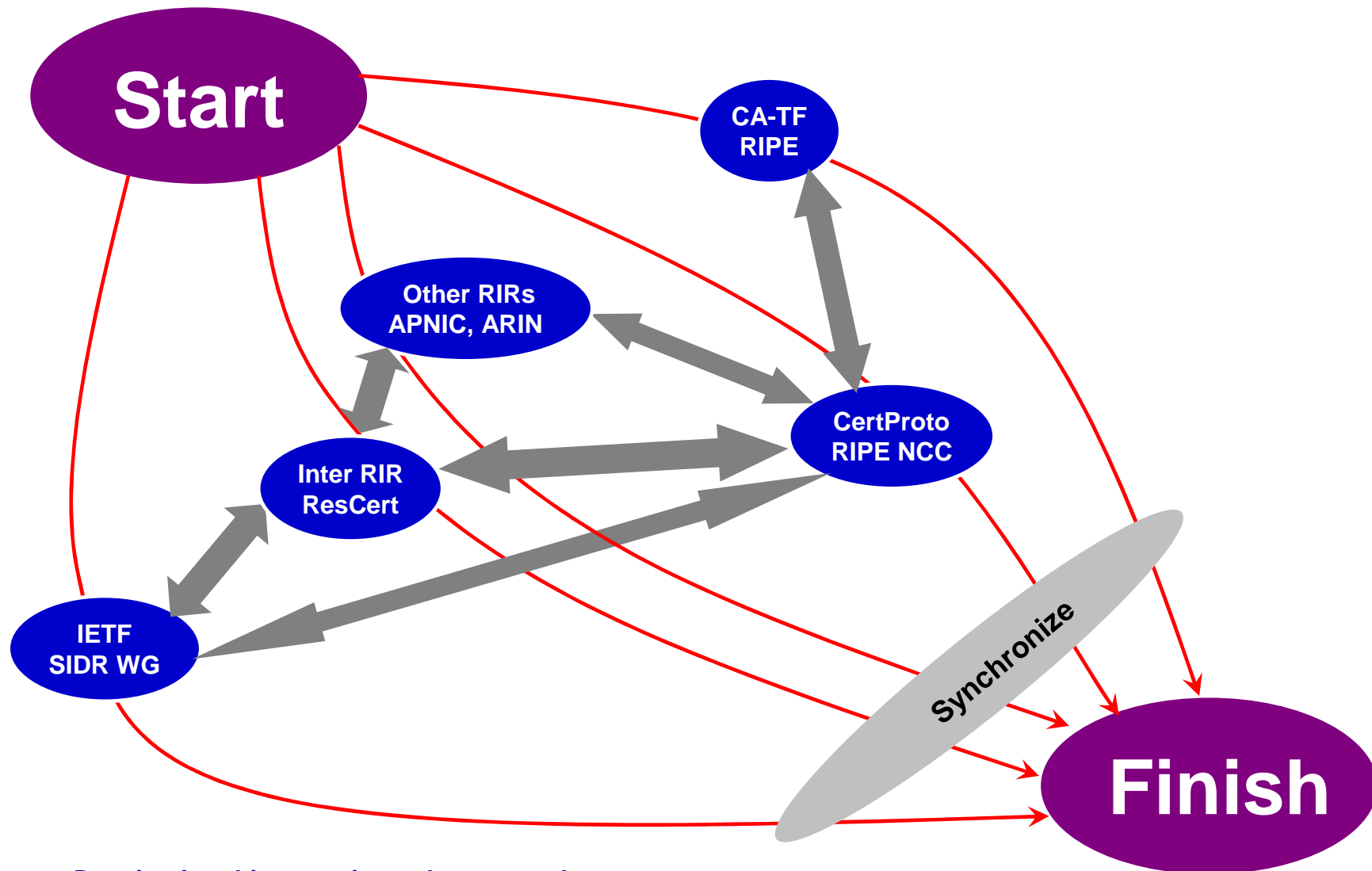
- Reaching this goal is complex and involves a lot of parties



Current efforts to reach this goal

- **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**
 - 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



Introduction

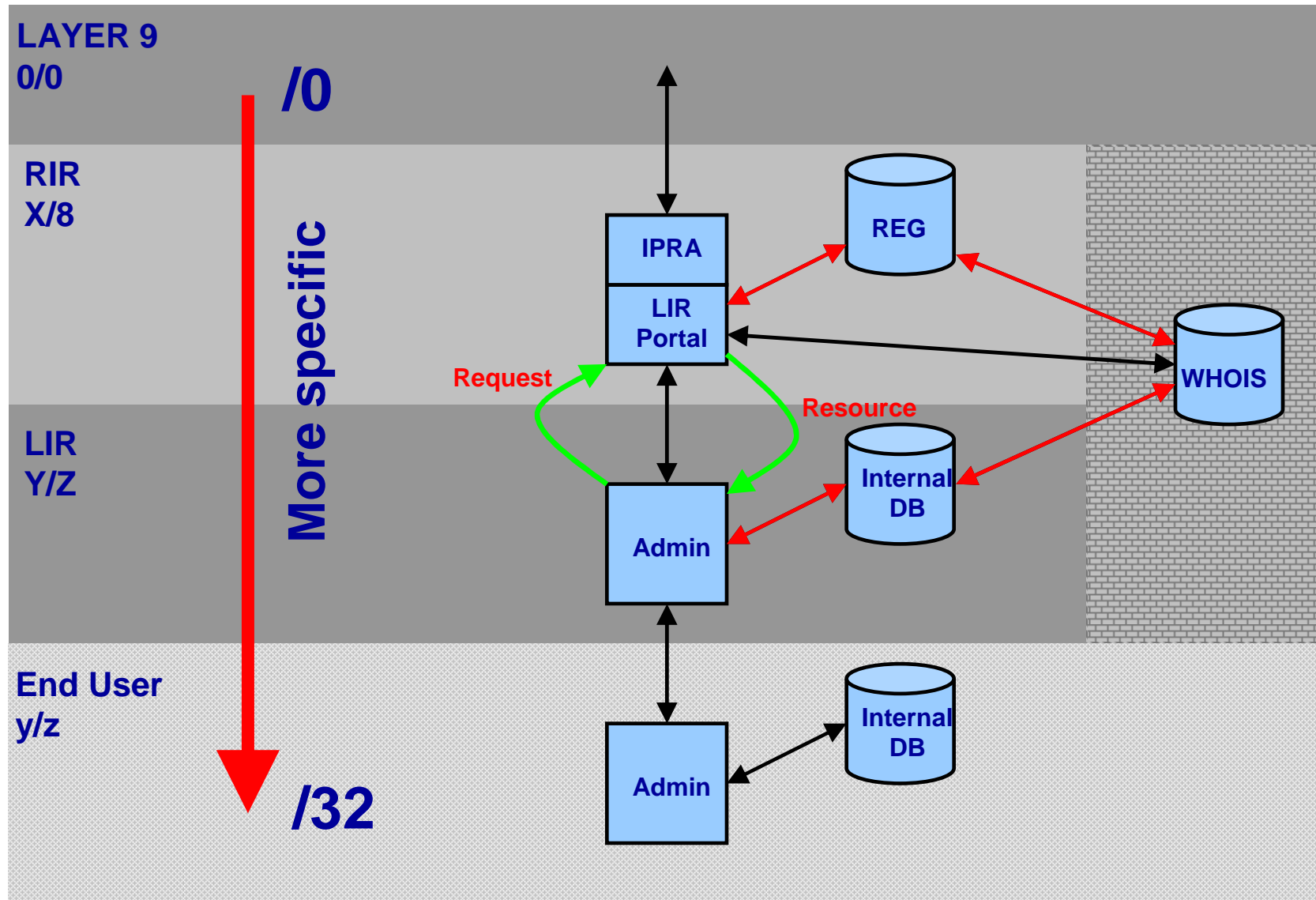
- Background
- Current view of the certification system
- RIPE NCC CertProto Project
- Conclusions



Current view of the system

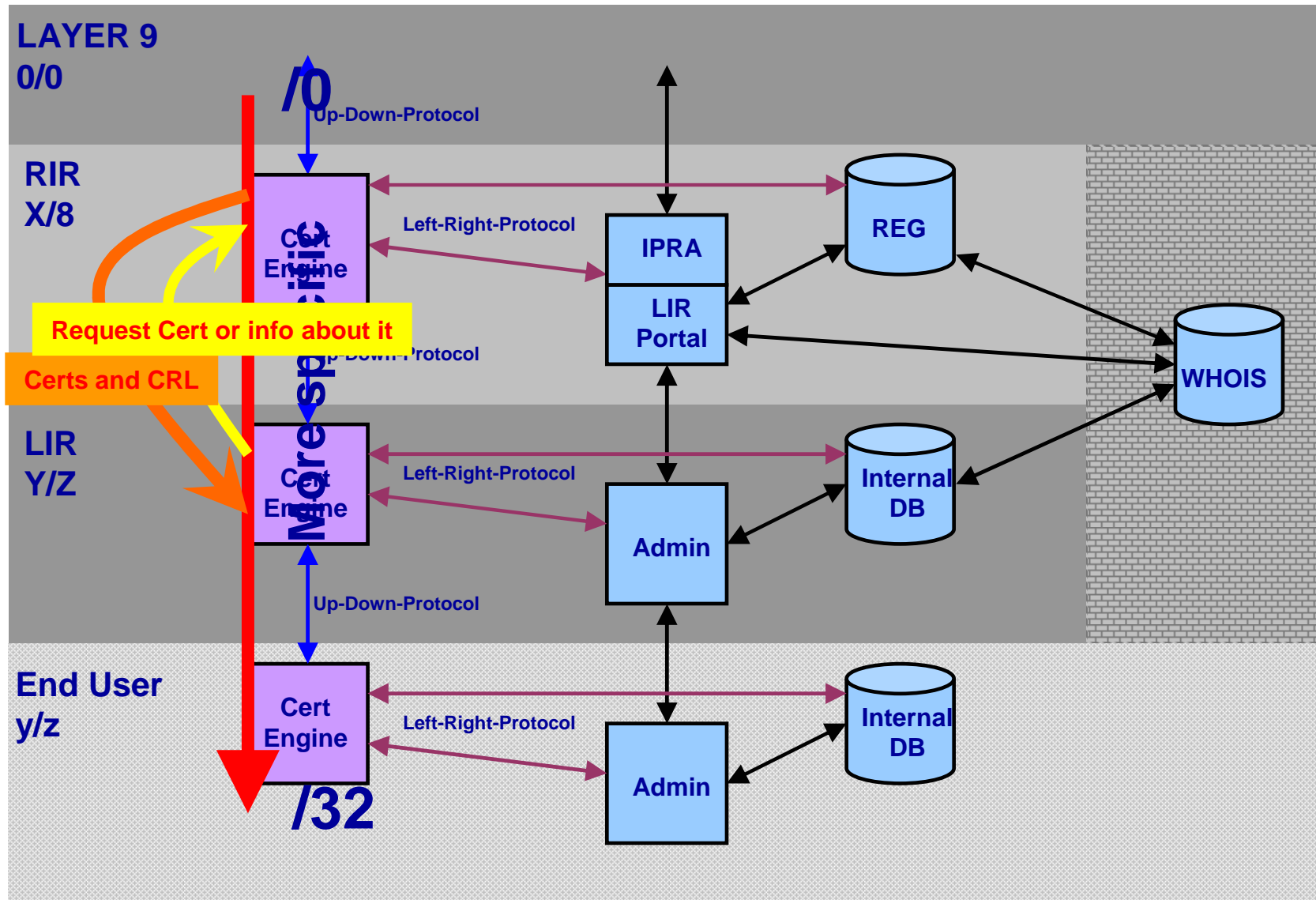
- System to hand out certificates
 - X.509 with IP/AS extensions (RFC 3779)
 - System runs in parallel with existing procedures
 - System uses existing technology as much as possible
- Functional layout
 - Extensive discussions between all parties
 - Rough consensus
 - Different implementations of elements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

Current situation

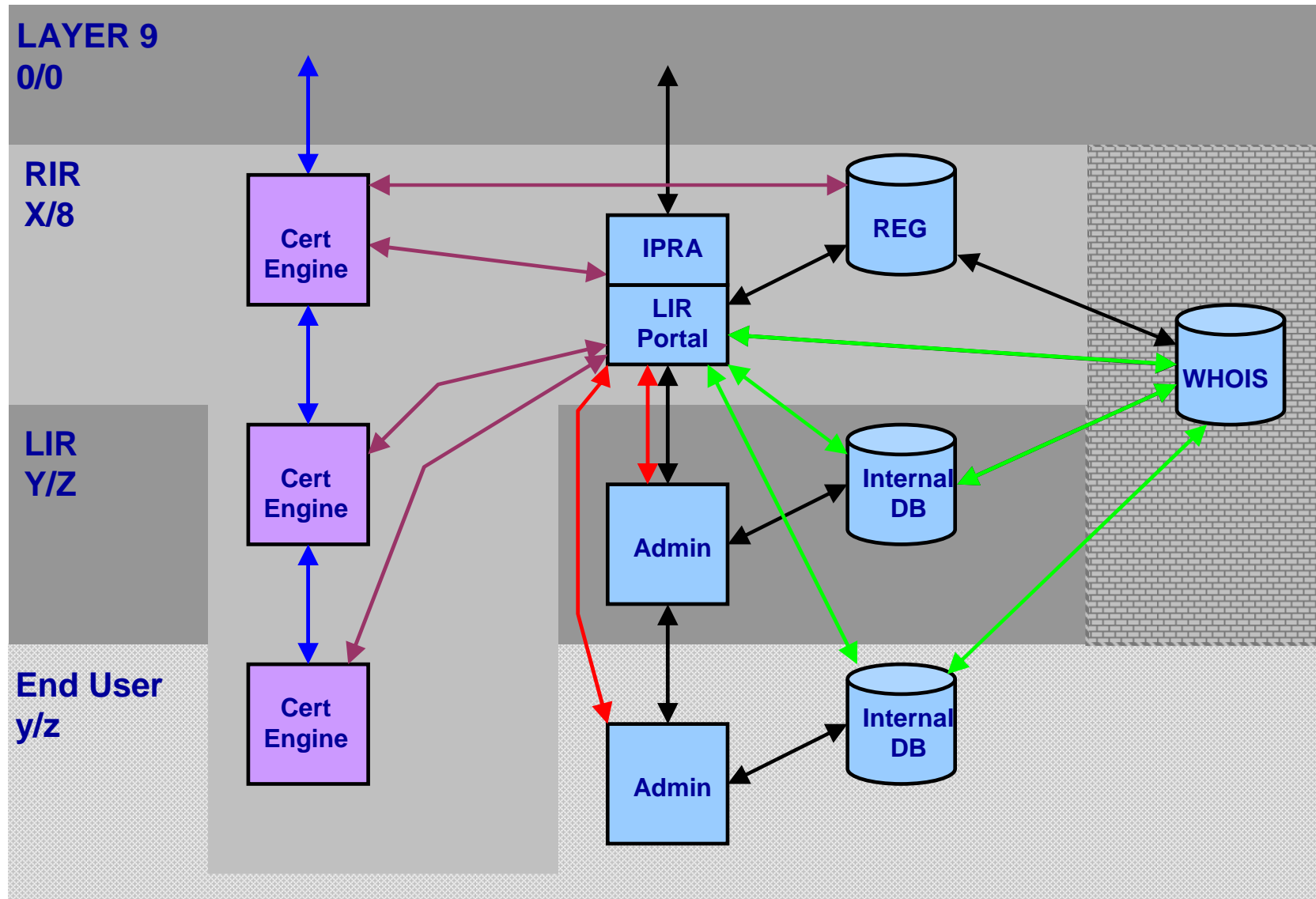




The future



Outsourced CA (aka hosted CA)





Introduction

- Background
- Current view of the certification system
- **RIPE NCC CertProto Project**
- Conclusions



RIPE NCC effort: CertProto Project

- Goals:
 - External: Enable the CA-TF to do their work
 - Internal: Understand all aspects of building and integrating a certification system for Internet resources before we actually start building it
- Milestones:
 - Build and deliver a prototype: 15/2 - 1/3
 - Report at RIPE 54 and get community feedback
 - Full report around 1 June for management review
 - Plan forward around 15 June



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
 - Policy
 - Together with TF, reported there
 - Prototype
 - Business Analysis/System Analysis
 - Data Accuracy
 - Accountability
 - Finance
 - Applications (after Monday...)
 - Collect and Review
 - Plan forward
- Jan-Apr '07**
- May '07**
- June '07**



Why did we build a prototype?

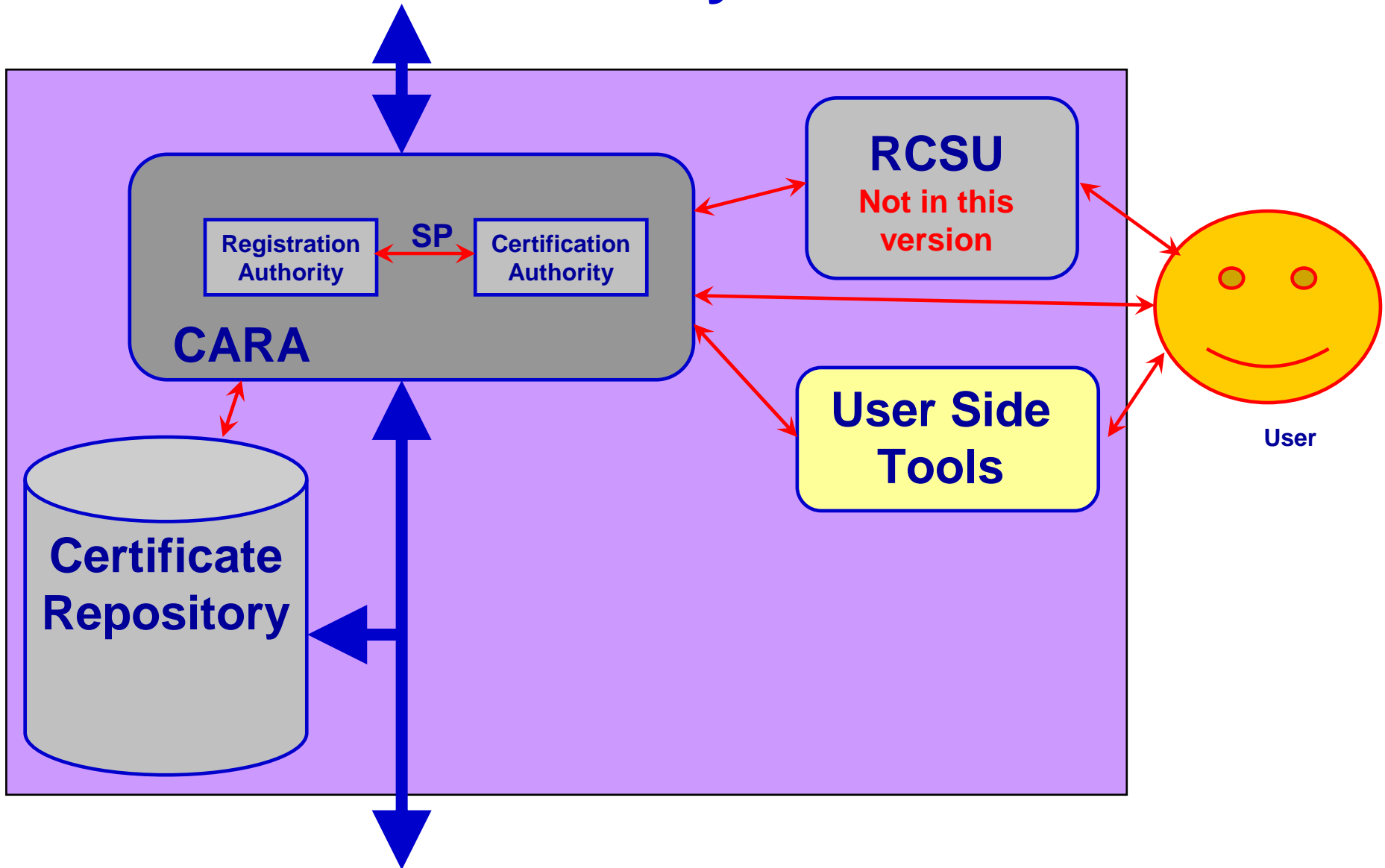
- Certification of Internet Resources:
 - X.509 well tested and understood
 - Application to Internet Resources is new
 - Lots of possibilities, options, ideas
- Little experience with the technology inside the NCC
 - Need something to gain hands-on experience
 - Need something tangible to test ideas and concepts
- Non goals:
 - Production level software
 - Shiny web interfaces



Building the prototype

- Built on assumptions
 - Correct at the time, but ideas have evolved since then
 - Standards were not defined
 - Business analysis had not been done
 - We may have to toss the prototype away after some time
- Defined a test plan, main factors:
 - Installation
 - Common operations based on expected usage
 - Usability and integration

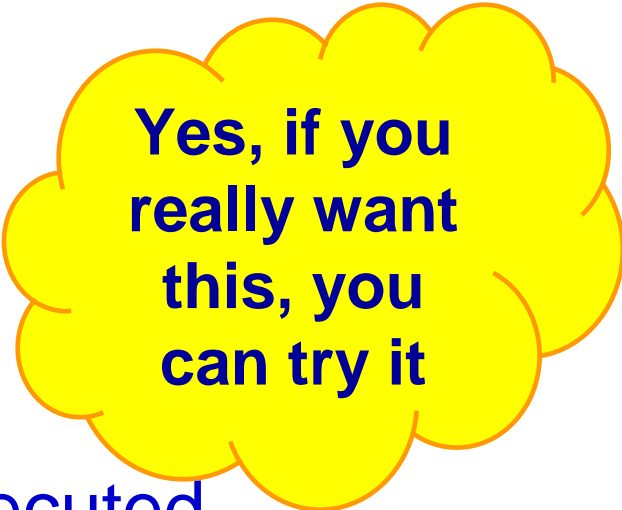
Overview of the system








In practice

- Delivered to
 - 3-4 external sites
 - Internal users
- Internal test plan successfully executed
- Conclusion:
 - This approach works
 - Too much hands on work for all parties
 - Reflected in design of full system
- Keep prototype running for a while
 - “As is”, no further development, no support



Yes, if you really want this, you can try it

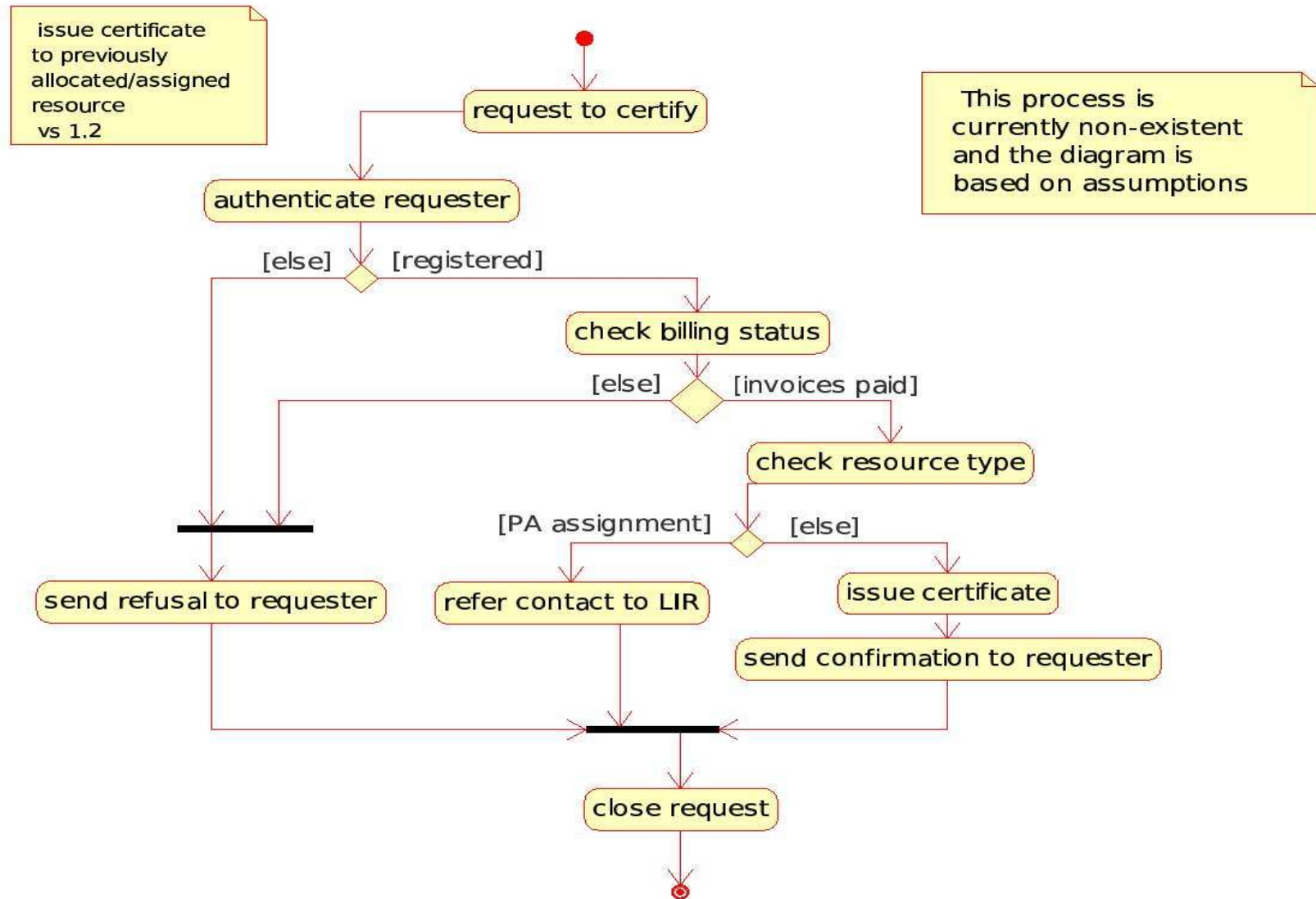




Business analysis & Systems analysis

- 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





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



Introduction

- Background
- Current view of the certification system
- RIPE NCC CertProto Project
- **Conclusions**



Plans

- Finish open work items
 - Accountability: DB versus real life
 - Financial aspects
 - Applications
- Collect all information
- Internal review: 1/6/2007
- Plan forward: 15/6/2007



Conclusions

- Various efforts to introduce certification of Internet resources
- Consensus on overall layout of the system
- CertProto at the RIPE NCC: well on its way to understand all consequences for introduction at the RIPE NCC

- More at RIPE 55



Questions? Discussion?

