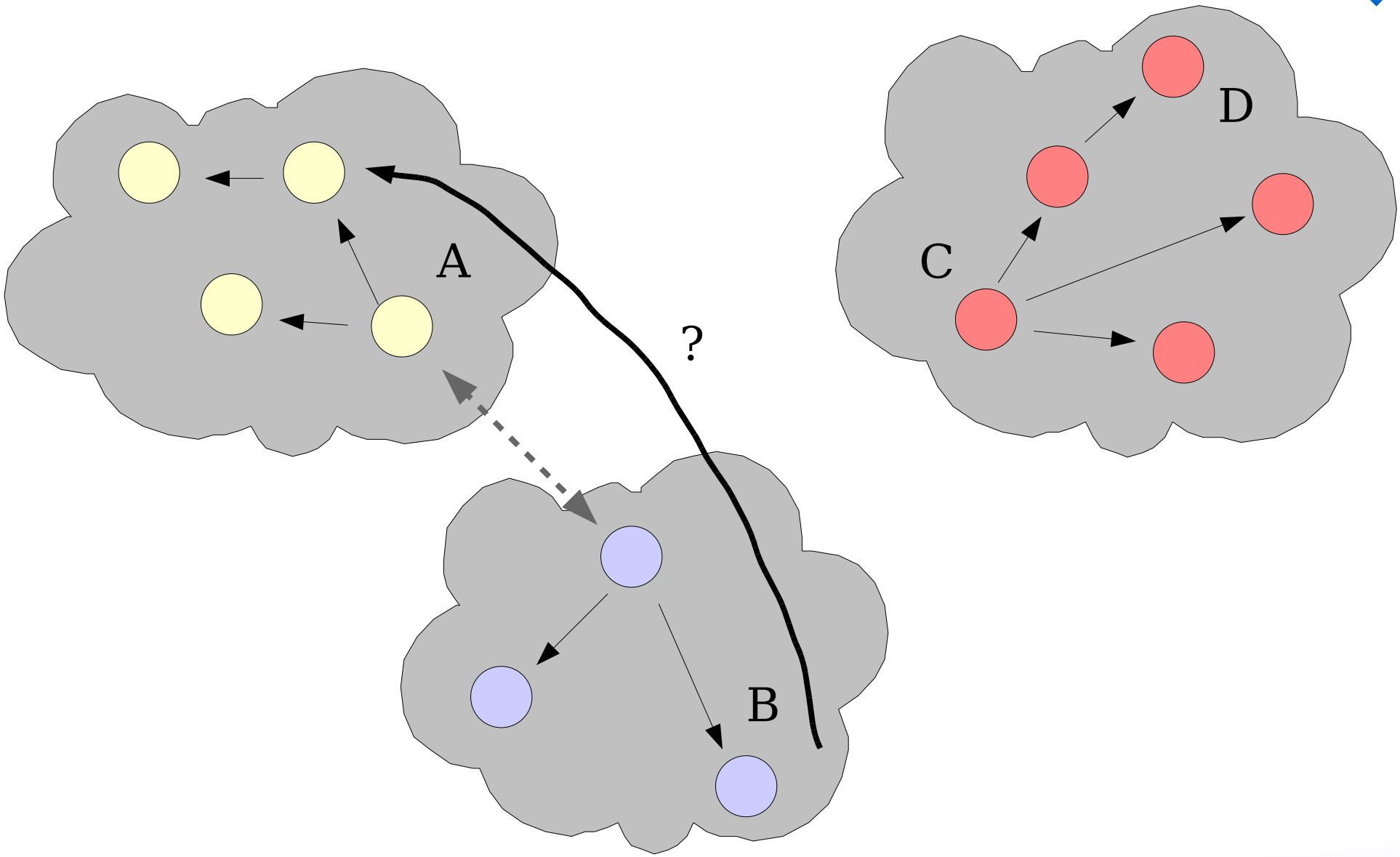
Massimiliano “Max” Pala <pala@cs.dartmouth.edu>
Project Manager <madwolf@openca.org>

PKI Resources Query Protocol

... or how to find PKI Resources (?)

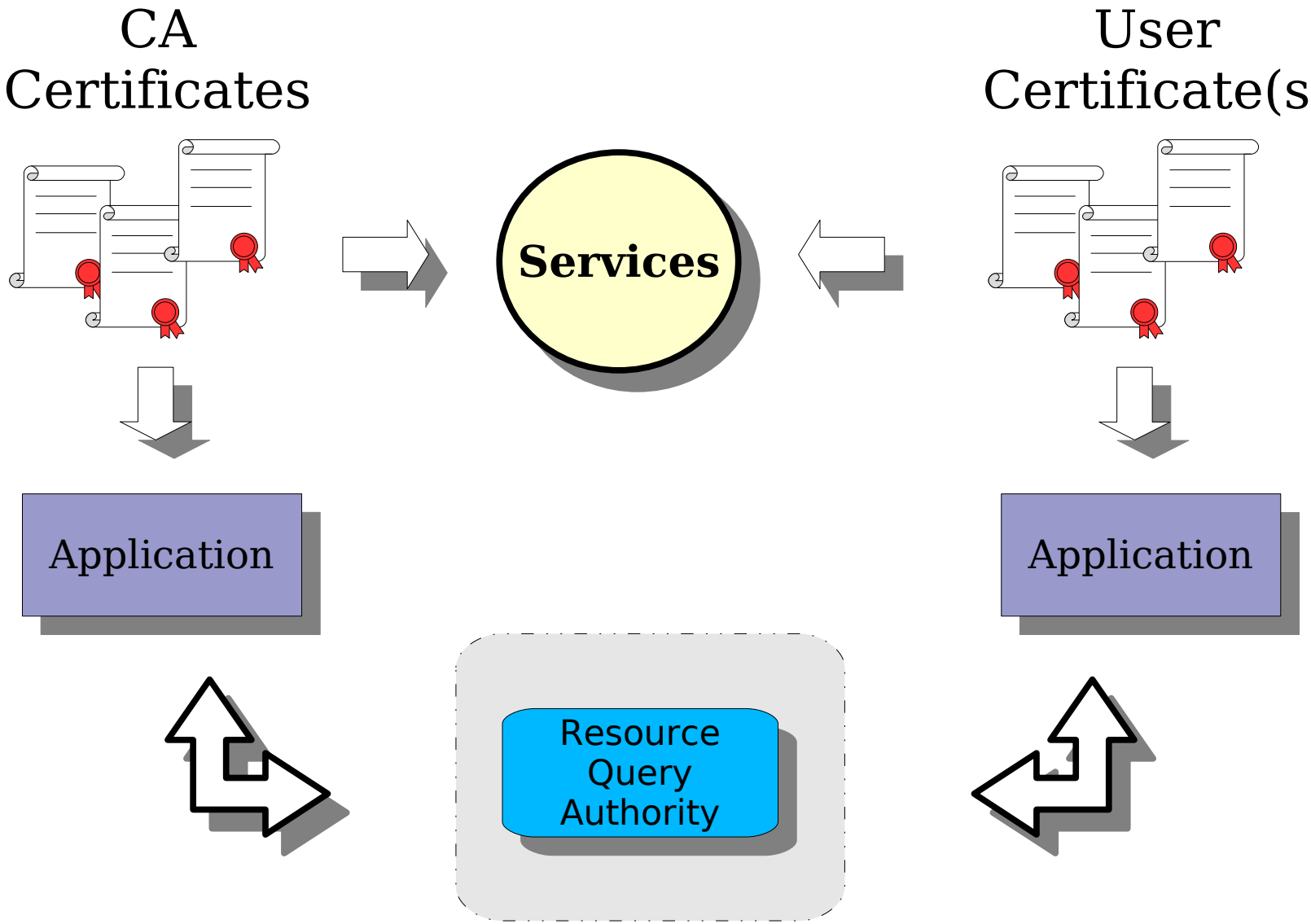
Path vs Resources Discovery



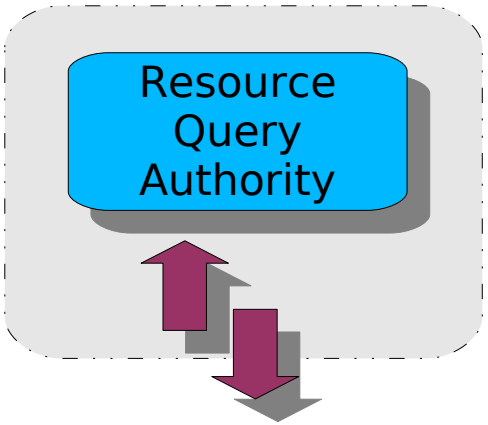
Simple Questions

- Where do I apply for a new Certificate from this CA ?
- Where do I apply for my Certificate Renewal by using CMS ?
- Where do I apply to get my Certificate revoked ?
- Where do I find the Certificates repository ?
- Where do I download the CP/CPS ?
- Where do I find the SCVP from `this` CA ?
- What services are provided by my CA now ?

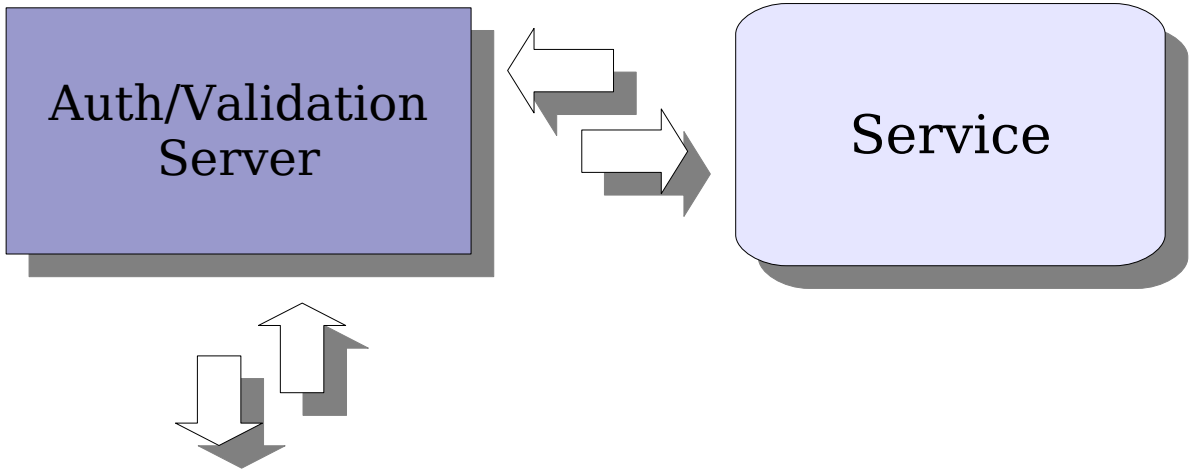
Example Scenario - 1



Example Scenario - 2



Additional step: PRQP is used to discover the URL of the Service(s) needed by the Auth/Validation Server (SCVP ?)



Client Certificate

Yes, We need a Solution!

- Finding resources to PKI resources is crucial
- Applications can provide simpler User Interfaces for users
  - ease configuration options
  - can take high-level trust decisions based on the level of security offered by available services or personal knowledge
- In some cross-organizations environments (Grids) even the distribution of simple CA information is a difficult task
- Everybody is doing things differently: we need to work on the matter and provide a specific (standardized) solution

What is PRQP (so far...)

- Simple client-server protocol
- Defines two type of messages
  - **PRQP Request**
  - **PRQP Response**
- Available as individual contribution
  - **I-D <pala-prqp-00.txt>**
- Updates will be available soon (January)
- Small changes in data structures (for response caching purposes)

What PRQP is not (so far...)

- A discovery System
- A data distribution System
- A validation Service (e.g., SCVP...)

But it can be used to get pointers to such services from a trusted authority!

The Proposed Solution

- Dynamic Solution
- Specific solution for the problem
- Ease roll-over of services (e.g, OCSP vs CRL)
- Ease Smart Cards or Hardware Tokens head-ache
- First building block:
  - **Eases interaction with CAs**
  - **More dynamic management of services**
  - **Opens up new possibilities for CAs**

Santa is Coming to town...

... And Xmas is coming along with many final calls ...

... can we think about adding a new PKIX WG item for the coming January ... ???

Contacts

- Dartmouth College
  pala@cs.dartmouth.edu
- OpenCA
  madwolf@openca.org

- Website
  http://www.openca.org/projects/prqpd
  http://www.openca.org/wiki/