PKI Resource Discovery Protocol (PRQP)

69th IETF Meeting

Chicago, IL, July 2007

Current Solutions

- Certificate Extensions
- DNS Records
- Webservices
- Local Network Oriented Solutions

PKI Simple Questions (?)

Where can I ask for a certificate revocation ?

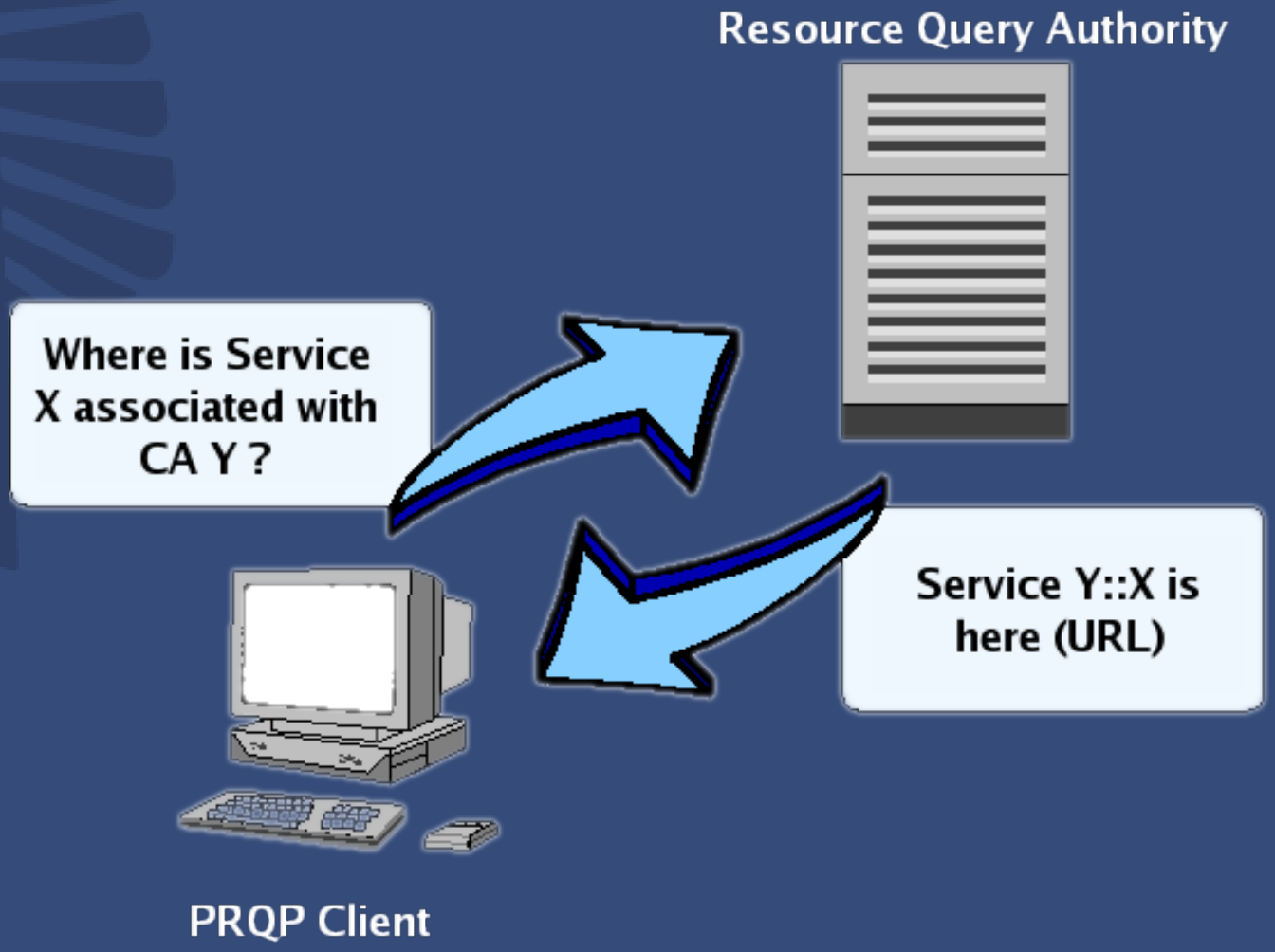
Where do I apply for a new Certificate ?

Where do I find the Certificates repository ?

The Proposed Solution

- The PKI Resources Query Protocol (PRQP)
- Allows a client to request URLs of Resources associated with a CA
- Provides “discovery” for any services (current and future):
  - Repositories (CRLs and Certs)
  - Validation Services (OCSP, SCVP, etc...)
  - Other Services (TimeStamping, Revocation, Subscription, etc...)
  - Future services

PRQP Basics


Resource Query Authority
Where is Service X associated with CA Y ?
Service Y::X is here (URL)
PRQP Client

PKI Resource Discovery

- Dynamic and simple Approach
  - Overcome staticity related to usage of AIA/SIA extensions
  - Allows for adding/removing pointers
  - One point of access for informations about resources (instead of CDP, AIA, SIA, etc...)
- Allows for Certificates not to be connected to a specific DNS domain
  - DNS based solutions (DNS SRV record approach) require a mapping between certs and DNS – not true for most of current CAs
- Enhance Interoperability across PKIs

Usage Scenarios

- *Rollover of services*
  - *a CA could require to move from one supported service to another without reissuing all certificates (DoD CRL problems)*
  - *Move to outsource services (third party provider)*
- *Fallback services*
  - *Adding and/or removing services without the need of having DNS/IP based re-routing*
- *Validation Services Implementation*
  - *SCVP (?)*

Thank You!

- *Contacts:*

  Massimiliano Pala (pala -at- cs.dartmouth.edu)
  OpenCA (project.manager -at- openca.org)
  IETF PKIX wg Mailing list

- Website:

  http://www.openca.org/projects/libprqp/

- Please read the draft (hopefully published soon) for full details!