

Dartmouth College

Massimiliano Pala <pala@cs.dartmouth.edu>



*Proposal for Deploying a PKI
Resource Query Authority*

*11th TF-EMC2 Meeting
9-10 July, 2008, Umea, Sweden*

Outline

- Introduction
 - Introduction & Motivations
 - Current Solutions & Limitations
- Protocol Details
 - PKI Resource Query Protocol
 - Resource Query Authority Deployment
- Conclusions
 - Implementation Details
 - Future Work

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 ?

PKI Resource Discovery

- Enhance Interoperability across PKIs
- Ease PKI Management Issues
 - Now connected to certificates' contents
- Foster simpler User Interfaces (UI)
 - User awareness Issues
- Usability of PKIs

Current Solutions

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

The Proposed Solution

- The PKI Resources Query Protocol
- Allows a client to request services and repositories URL 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

Status of PRQP

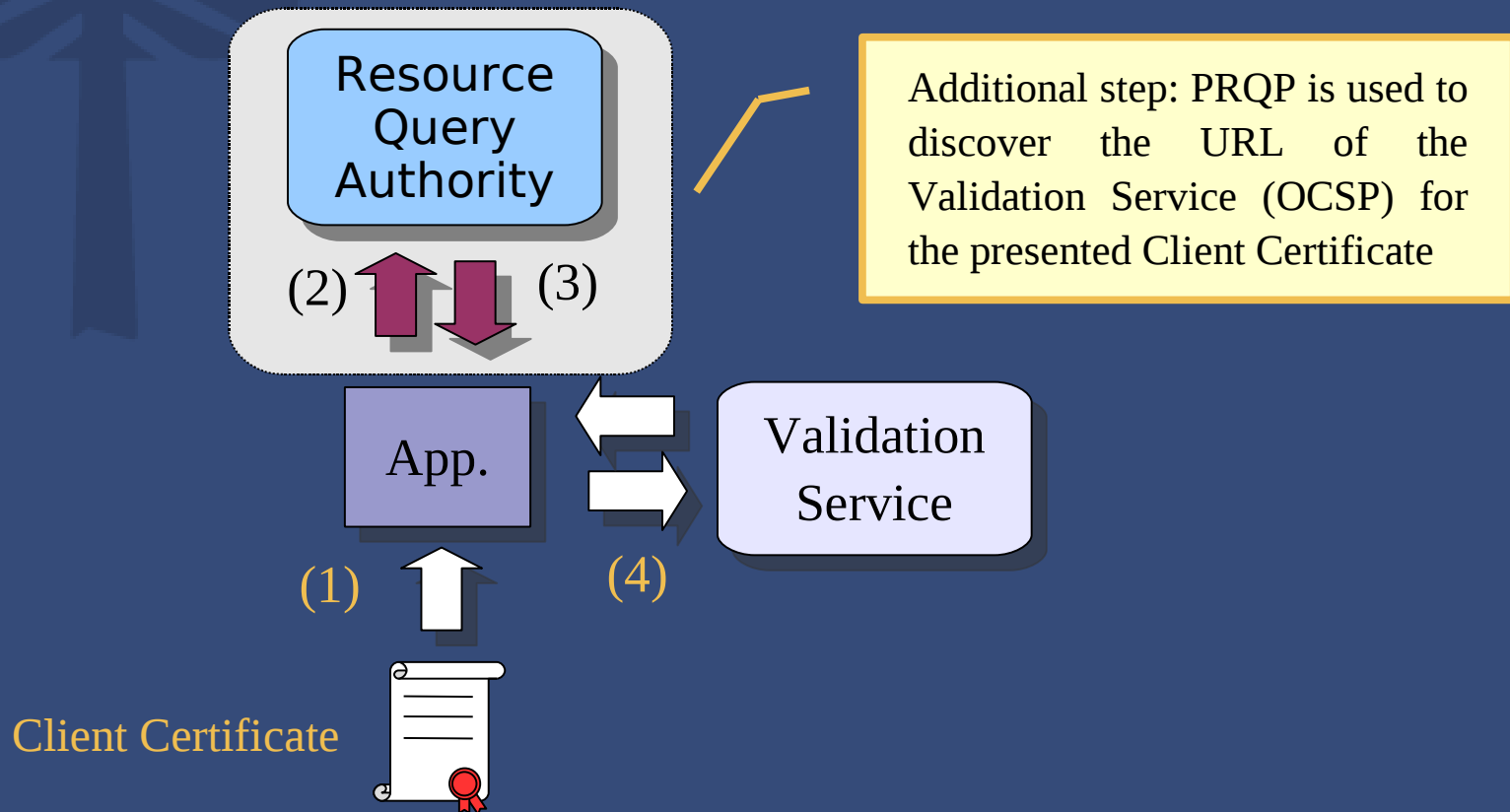
- The **PKI Resources Query Protocol (PRQP)** is undergoing the final call to be accepted as a working item of the PKIX work group (IETF)
- The I-D is currently available as <draft-pala-prqp-01.txt> from IETF
- We hope to push PRQP on the standard track as soon as possible

PRQP in a “Nut”Shell

- Simple client-server protocol
- The server is the **Resource Query Authority**
 - It is certified by a CA to provide PRQP responses (exactly as an OCSP is authorized to provide OCSP responses)
 - Can provide responses for multiple CAs
 - Trusted Mode
 - Multiple Certificates from different Cas
- “Where can I find service “X” related to CA “Y”
 - “Service “X” from CA “Y” can be found at this URL

The Request Query Authority

- Authority designated to answer to PKI Resource Location



Examples

- PKIX Services
 - id-ad-prqp
 - id-ad-prqp-ocsp
 - id-ad-prqp-calssuers
 - id-ad-prqp-timestamping
 - Id-ad-prqp-dvcs
 - Id-ad-prqp-caRepository
- HTTP (Browser) services
 - id-ad-prqp-http-certs --- HTTP cert repository
 - id-ad-prqp-http-crls --- HTTP CRL URL
 - id-ad-prqp-xkmsGateway --- XKMS Gateway
 - id-ad-prqp-cmsGateway --- CMS Gateway

Examples (2)

- Certificate Policies
 - Id-ad-prqp-certPolicy --- Certificate Policy (CP) URL
 - Id-ad-prqp-certPracticesStatement --- Certification Practices Statement (CPS) URL
- Level Of Assurance
 - id-ad-prqp-certLOAPolicy --- LOA Policy URL
 - id-ad-prqp-certLOAlevel --- Certificate LOA Modifier URL
- HTTP (Browsers) based services
 - id-ad-prqp-httpRevokeCertificate --- HTTP Based Certificate Revocation Service
 - id-ad-prqp-httpRequestCertificate --- HTTP Based Certificate Request Service

Examples (3)

- Grid Specific Services
 - Id-ad-prqp-grid-accreditationBody --- CA Accreditation Body(s)
 - id-ad-prqp-grid-accreditationPolicy --- CA Accreditation Policy Document(s)
 - id-ad-prqp-grid-accreditationStatus --- CA Accreditation Status Document(s)
 - id-ad-prqp-grid-commonDistributionUpdate --- Grid Distribution Package(s)
 - id-ad-prqp-grid-accreditedCACerts --- Certificates of Currently Accredited CAs
 - Id-ad-prqp-certPolicy --- Certificate Policy (CP) URL
 - Id-ad-prqp-certPracticesStatement --- Certification Practices Statement (CPS) URL

Deployment Plans

- TACAR provides trusted certificate repository and information for many CAs
- We propose to run an RQA that will provide support for all the TACAR's CAs
- The Server will be hosted at Dartmouth College
- Two Options
 - Operating as a Trusted Responder
 - Getting a Certificate from each CA that wish to participate in TACAR's RQA
- We will need to define the policies for CAs admins to update information related to their CAs
 - Probably by using an authenticated upload (web) form
- A web-based client will be setup

Implementation Details

- PRQP API included into LibPKI (v0.1.9)
 - Provides easy-to-use functionality
 - PRQP_REQUEST_new_cacert_file()
- Available for any Unix based system (eg., Linux, Solaris8-10, OpenSolaris, BSD, MacOS, iPhoneOS2.0, etc...)
- PRQP Server (available version at OpenCA)
 - Based on OpenCA OCSPD
 - Implements PRQP over HTTP
 - Supports multiple CA

Conclusions

- PRQP provides/is:
 - Dynamic Solution
 - Fast and easy to implement
 - Specific solution for the problem
 - Ease rollover of services
 - Supported in LibPKI (Easy-to-use PKI library)
- Initial support for a PKI Discovery Infrastructure for TACAR
 - Allow writing applications that make use of the deployed infrastructure
 - Provide us with valuable feedback to improve current specification

Future Works

- PKI ***Usability and Interoperability project*** at Dartmouth College:
 - Extending the PRQP to a Peer-2-Peer Authenticated Network (for inter-federation PRQP support)
 - Already published a paper at EuroPKI (PEACHES and Peers)



Questions ?



Thank You!

- Contacts:

Massimiliano Pala <pala@cs.dartmouth.edu>

OpenCA <project.manager@openca.org>

- Website

<http://mm.cs.dartmouth.edu/prqp/> (DEMO)

<https://www.openca.org/projects/prqpd/>