PKI Resources Query Protocol
Status Update

Massimiliano Pala <pala@cs.dartmouth.edu>
OpenCA Project Manager <project.manager@openca.org>
Outline

- Document Updates
  - Editorial Changes
  - New Sections

- Current Activities
  - Deployment of PRQP in TACAR

- Future Plans for PRQP
  - Integration with TAMP
PRQP & Document Status

- Last published version -00

Recent Document Activities
- **Definition of new OIDs**
- **Text for defined OIDs and their meaning** *(more on this later)*

To ease PRQP deployment
- **Adding section on how to provide clients with RQAs addresses**
  - DHCP
  - DNS SRV records
Updated Data Structures

Changes in the Response Token

ResourceResponseToken ::= SEQUENCE {
    serviceId OBJECT IDENTIFIER,
    ResourceLocator [0] EXPLICIT SEQUENCE OF IA5String,
    Version [1] INTEGER OPTIONAL,
    TextInfo [2] UTF8String OPTIONAL
}

Eliminated ResourceInfo

ResourceInfo ::= SEQUENCE {
    resourceUri IA5String,
    -- resource locator
    version [0] INTEGER OPTIONAL,
    -- version of the protocol or data format
}
Updated OIDs

- Fixed and ambiguity in ADs for browser-based services (data format vs transport protocol)

--- HTML (Browsers) based services
id-ad-prqp-htmlRevokeCertificate
  OBJECT IDENTIFIER ::= {id-ad-prqp 30}
--- HTML Based Certificate Revocation Service
id-ad-prqp-htmlRequestCertificate
  OBJECT IDENTIFIER ::= {id-ad-prqp 31}
--- HTML Based Certificate Request Service
id-ad-prqp-htmlRenewCertificate
  OBJECT IDENTIFIER ::= {id-ad-prqp 32}
--- HTML Based Certificate Renewal Service
id-ad-prqp-htmlSuspendCertificate
  OBJECT IDENTIFIER ::= {id-ad-prqp 33}
--- HTML Based Certificate Suspension Service
Updated OIDs (cont.)

- Added two new Service OIDs

- TAMP service
  
  ```
  --- Trust Anchor Management Services
  id-ad-prqp-tampUpdate OBJECT IDENTIFIER ::= {id-ad-prqp 70}
  ```

- CA Incident Report
  
  ```
  --- Risk Management Services
  id-ad-prqp-caIncidentReport
  
  OBJECT IDENTIFIER ::= {id-ad-prqp 90}
  ```
PRQP Deployment Activities
PRQP Deployment for TACAR

- PRQP Deployment for TACAR CAs
  - Dartmouth College will run a Trusted RQA

- TACAR project
  - provides a trusted repository of CA certificates and Certificate Practice Statements

- Participating Bodies
  - EuGridPMA
  - IGTF
  - EduGain
  - Others
PRQP Deployment: status

- Slow progress due to lack of resources

- Agreed on Operational Protocol for Phase I
  - RQA operators procedure

- Deployment Agenda
  - RQA running in PTA - December 2008
  - RQA in authorized mode - March 2008
  - Integration with Browsers - February 2008
Considerations and Future Work

- Speed up the deployment of PRQP for TACAR
- Interactions with other PKIX work
  - TAMP and PRQP to provide usable TAM (next slide)
- Still no progress on DHCP interaction
  - RQA service entry for DHCP and DHCPv6
- Future work
  - Move forward with the P2P specification for PRQP deployment (PRQP I-D section A.2)
PRQP and TAMP

- PRQP can enable Organizations to endorse
  - Its own TAM service
  - Externally provided services

- Provide multiple pointers to external TAM service
  - Trust between the TAM provider and the client must exists or shall be established

- Background
  - One or more TA present in the application
    - Mozilla Corp. for Firefox
    - Microsoft and Verisign for IE
    - Your organization's CA certificate for any app
User Interface Example

- PRQP can enable a dialog similar to the following:

![Security Question Dialog]

Trust Decision Required

Do you want to add the Trust Anchor Management Operators endorsed by your Trusted Authorities?

Allow only: Authorities that issued me a certificate

- Yes, do it
- No, don't allow
- Advanced...
User Interface Example

Where is the CA TAM service

PRQP Server

Application

Organization CA

Microsoft TAMP Service

Mozilla TAMP Service
Questions & Contacts

- Dartmouth College
  pala@cs.dartmouth.edu

- OpenCA
  project.manager@openca.org

- TACAR project
  http://www.tacar.org

- Website
  http://www.openca.org/projects/prqpd
  http://www.openca.org/wiki/
PKI Resource Discovery Protocol

PRQP defines the message format between a client and a server.

Resource Query Authority

CMS Gateway for CA₁ is at http://.../...

Where is the CMS Gateway associated with CA₁

Client Application (or OS ???)