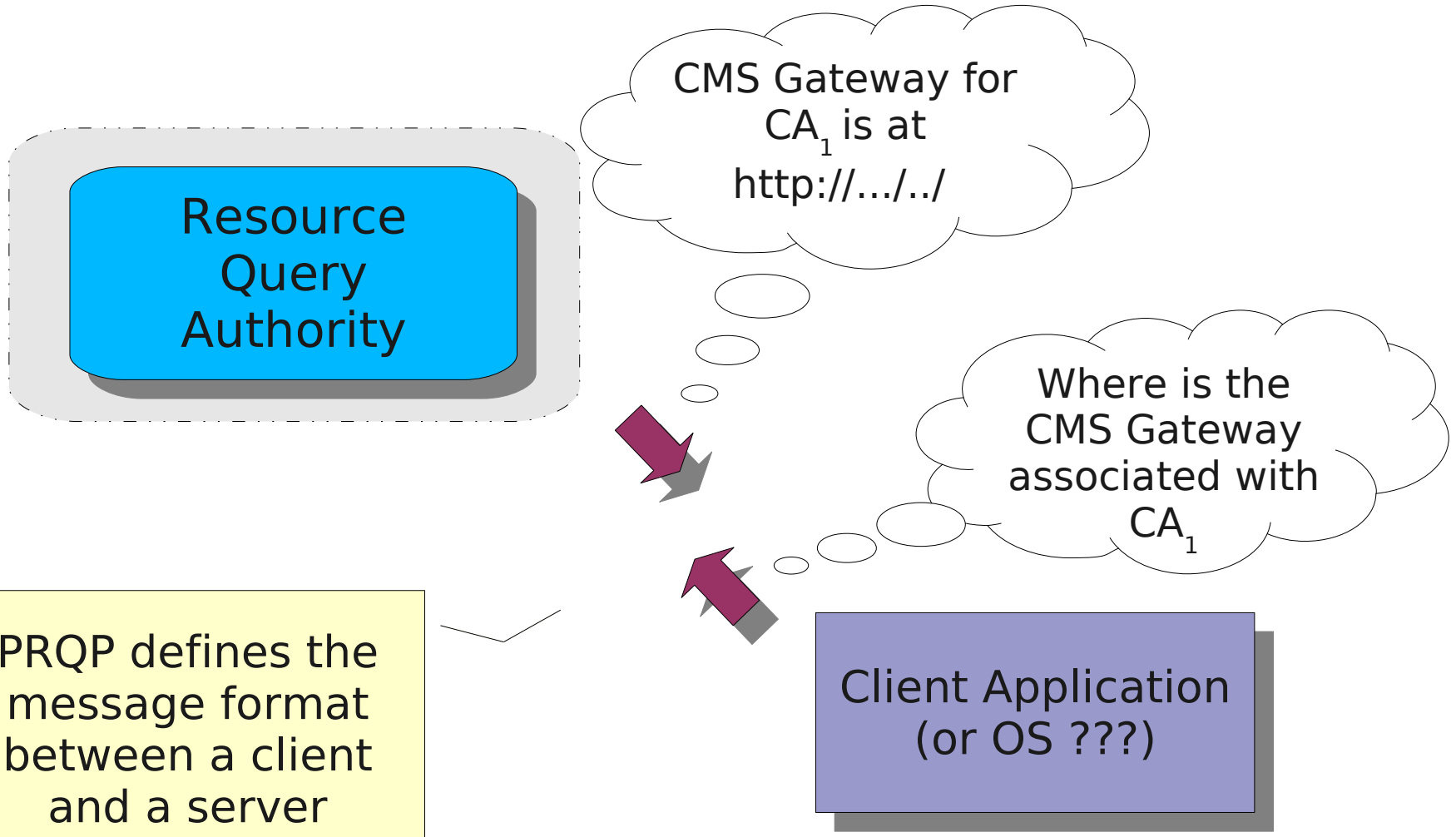
PKI Resources Query Protocol
Status Update & Recent Activities

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

PKI Resource Discovery Protocol



PRQP & Document Status

- PKIX ID on Experimental Track
  - **draft-ietf-pkix-prqp-00.txt (Jul 2008)**
  - **Added and re-organized the OIDs**
  - **We need to provide more document about defined OIDs and their meaning**
- Issue Faced
  - **Lack of OIDs to identify current services (e.g., which OID identifies an SCVP service ?)**
- Suggestion
  - **guidelines for future PKIX documents on OIDs. (eg. to specify an id-ad or id-ad-prqp) ?**

Updated OIDs (1/4)

```
id-kp-PRQPSigning        OBJECT IDENTIFIER ::= { id-kp 10 }
       --- extended Key Usage for PRQP purposes

id-prqp                  OBJECT IDENTIFIER ::= { id-pkix 23 }
id-prqp-pta              OBJECT IDENTIFIER ::= { id-prqp 1 }
       --- PRQP Trusted Authority
id-ad-prqp                        OBJECT IDENTIFIER ::= {id-ad 12 }
       --- Access Descriptor for PRQP

id-ad-prqp-ocsp                   OBJECT IDENTIFIER ::= {id-ad-prqp 1}
id-ad-prqp-caIssuers              OBJECT IDENTIFIER ::= {id-ad-prqp 2}
id-ad-prqp-timestamping           OBJECT IDENTIFIER ::= {id-ad-prqp 3}
id-ad-prqp-scvp                   OBJECT IDENTIFIER ::= {id-ad-prqp 4}

id-ad-prqp-caRepository           OBJECT IDENTIFIER ::= {id-ad-prqp 5}
id-ad-prqp-http-certs             OBJECT IDENTIFIER ::= {id-ad-prqp 6}
        --- HTTP certificate repository
id-ad-prqp-http-crls              OBJECT IDENTIFIER ::= {id-ad-prqp 7}
        --- HTTP CRL download URL
```

Updated OIDs (2/4)

```
id-ad-prqp-xkmsGateway          OBJECT IDENTIFIER ::= {id-ad-prqp 10}
        --- XKMS Gateway
id-ad-prqp-cmsGateway           OBJECT IDENTIFIER ::= {id-ad-prqp 11}
        --- CMS Gateway
id-ad-prqp-scepGateway          OBJECT IDENTIFIER ::= {id-ad-prqp 12}
        --- SCEP Gateway

--- Certificate Policies
id-ad-prqp-certPolicy           OBJECT IDENTIFIER ::= {id-ad-prqp 20}
        --- Certificate Policy (CP) URL
id-ad-prqp-certPracticesStatement
                                OBJECT IDENTIFIER ::= {id-ad-prqp 21}
        --- Certification Practices Statement (CPS) URL

--- Level Of Assurance
id-ad-prqp-certLOAPolicy        OBJECT IDENTIFIER ::= {id-ad-prqp 25}
        --- LOA Policy URL
id-ad-prqp-certLOALevel         OBJECT IDENTIFIER ::= {id-ad-prqp 26}
        --- Certificate LOA Modifier URL
```

Updated OIDs (3/4)

```
--- HTTP (Browsers) based services
id-ad-prqp-httpRevokeCertificate
                                OBJECT IDENTIFIER ::= {id-ad-prqp 30}
        --- HTTP Based Certificate Revocation Service
id-ad-prqp-httpRequestCertificate
                                OBJECT IDENTIFIER ::= {id-ad-prqp 31}
        --- HTTP Based Certificate Request Service
id-ad-prqp-httpRenewCertificate
                                OBJECT IDENTIFIER ::= {id-ad-prqp 32}
        --- HTTP Based Certificate Renewal Service
id-ad-prqp-httpSuspendCertificate
                                OBJECT IDENTIFIER ::= {id-ad-prqp 33}
        --- Certificate Suspension Service

--- Webdav Services
id-ad-prqp-webdavCert           OBJECT IDENTIFIER ::= {id-ad-prqp 40}
        --- Webdav Certificate Validation
id-ad-prqp-webdavRev            OBJECT IDENTIFIER ::= {id-ad-prqp 41}
        --- Webdav Certificate Revocation
```

Updated OIDs (4/4)

```
--- Grid Specific Services
id-ad-prqp-grid-accreditationBody
                                OBJECT IDENTIFIER ::= {id-ad-prqp 50}
        --- CA Accreditation Body(s)
id-ad-prqp-grid-accreditationPolicy
                                OBJECT IDENTIFIER ::= {id-ad-prqp 51}
        --- CA Accreditation Policy Document(s)
id-ad-prqp-grid-accreditationStatus
                                OBJECT IDENTIFIER ::= {id-ad-prqp 52}
        --- CA Accreditation Status Document(s)
id-ad-prqp-grid-commonDistributionUpdate
                                OBJECT_IDENTIFIER ::= {id-ad-prqp 53}
        --- Grid Distribution Package(s)
id-ad-prqp-grid-accreditedCACerts
                                OBJECT IDENTIFIER ::= {id-ad-prqp 54}
        --- Certificates of Currently Accredited CAs
```

PRQP Deployment (1/2)

- 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

- Two operational Phases
- Phase I (test)
  - **The RQA will run in Trusted Mode**
- Phase II (operational)
  - **Participating CAs will issue the RQA a certificate to act as an authorized responder for their CA**

Conclusions

- Deployment of PRQP for TACAR
- Interactions with other PKIX work
  - **TAM**
  - **SCVP**
- Consider Interactions with external work
  - **RQA service entry for DHCP and DHCPv6**
  - **RQA service entry for DNS SRV**
- Future work
  - **Move forward with the P2P specification for PRQP deployment (PRQP I-D section A.2)**

Questions & Contacts

- Dartmouth College
  pala@cs.dartmouth.edu
- OpenCA
  madwolf@openca.org
- TACAR project
  http://www.tacar.org
- Website
  http://www.openca.org/projects/prqpd
  http://www.openca.org/wiki/