

# PKI Resources Query Protocol Deployment

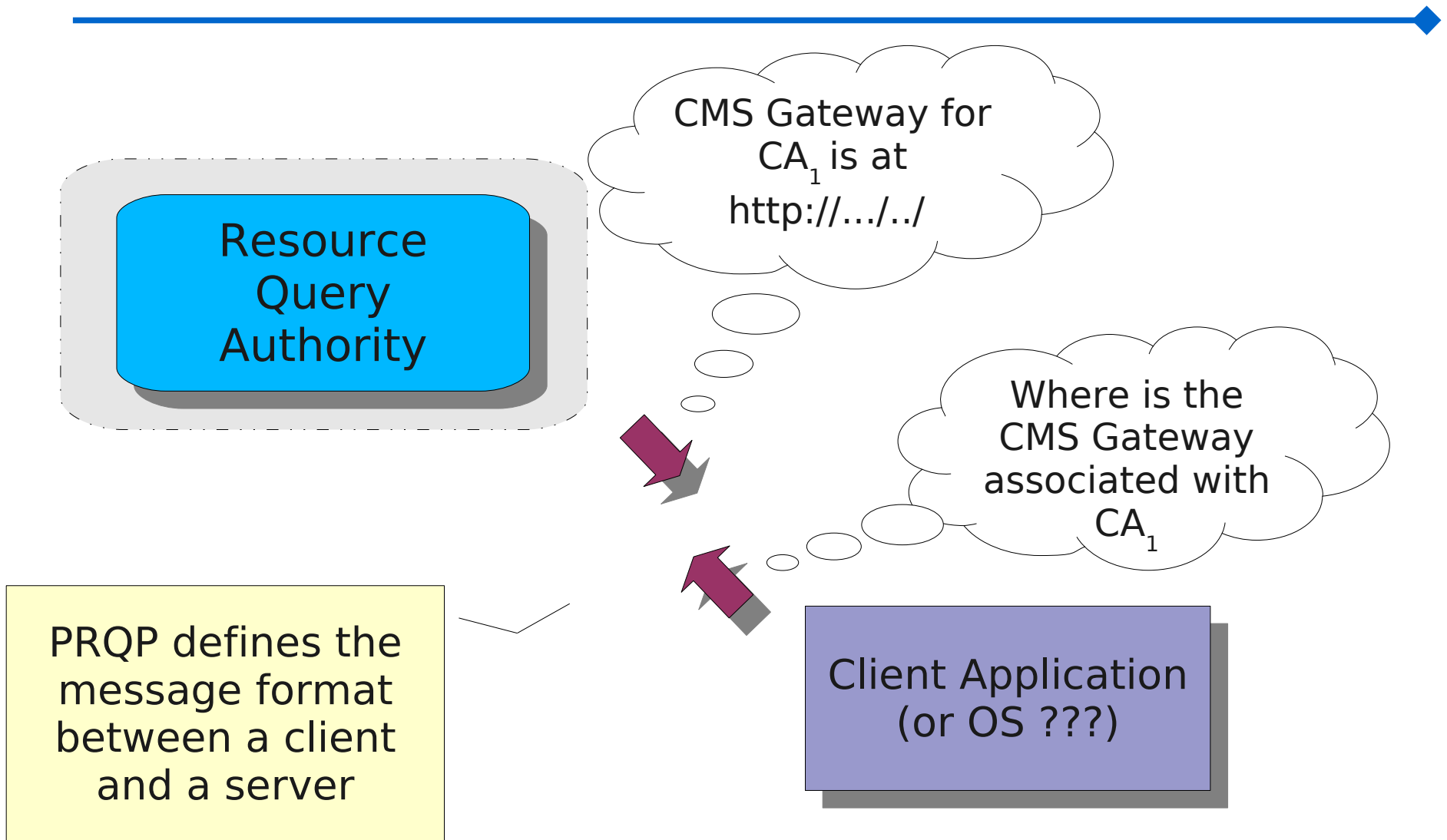
Massimiliano Pala <[pala@cs.dartmouth.edu](mailto:pala@cs.dartmouth.edu)>  
OpenCA Project Manager <[project.manager@openca.org](mailto:project.manager@openca.org)>

# PKI Resources Discovery

---

- Pointers to Resources
  - **Extensions in Certificate**
  - **Ad-Hoc Configurations in Apps**
  - **Advertise them on the CA's web pages**
- The PKI Resource Query Protocol
  - **Working Item at PKIX WG**
  - **Experimental Track**

# PKI Resource Discovery Protocol



# PRQP & Document Status

---

- Simple client-server protocol
- Defines two type of messages
  - **PRQP Request**
  - **PRQP Response**
- Updated beginning of 2010 (v04)
  - **Small Fixes**
  - **Addition of new OIDs for Grid Services**

# Updated OIDs

	OID	Text	Description
PKIX	id-ad 1	ocsp	OCSP Service
	id-ad 2	caIssuers	CA Information
	id-ad 3	timeStamping	TimeStamping Service
	id-ad 10	dvcs	DVCS Service
	id-ad 11	scvp	SCVP Service
General PKI Operations	id-ad 50	certPolicy	Certificate Policy (CP) URL
	id-ad 51	certPracticesStatement	Certification Practices Statement (CPS) URL
	id-ad 60	httpRevokeCertificate	HTTP Based (Browsers) Certificate Revocation Service
	id-ad 61	httpRequestCertificate	HTTP Based (Browsers) Certificate Request Service
	id-ad 62	httpRenewCertificate	HTTP Based (Browsers) Certificate Renewal Service
	id-ad 63	httpSuspendCertificate	Certificate Suspension Service
	id-ad 40	cmsGateway	CMS Gateway
	id-ad 41	scepGateway	SCEP Gateway
	id-ad 42	xkmsGateway	XKMS Gateway
	eng-ltd 3344810 10 2	webdavCert	Webdav Certificate Validation Service
	eng-ltd 3344810 10 3	webdavRev	Webdav Certificate Revocation Service
Grid	id-ad 90	accreditationBody	Accreditation Body URL
	id-ad 91	accreditationPolicy	Accreditation Policy
	id-ad 92	accreditationStatus	Accreditation Status Document
	id-ad 95	commonDistributionUpdate	Grid Distribution Package
	id-ad 96	accreditedCACertificates	Certificates of Currently Accredited CAs

# Deployment in TACAR

---

- TACAR Project
  - **TERENA Academic CA Repository**
  - **Identification/authorisation procedures**
  - **Most of the EuGridPMA root CAs**
  - **National Research and Education Networks**
- PRQP Management included in the new CA Management Panel
- Server hosted at Dartmouth College
  - **Certificate Issued by TERENA's CA**
  - **Responder for all TACAR's CA**

# Deployment in FBPKI

---

- Initial Deployment in ICAM test lab
  - **Open Source Software**
  - **Evaluation for deploying the protocol within the FBPKI architecture**
- Just Started!
  - **Expect some news in the next few months**

# Available Software

---

- Open Source implementation (PRQPD) available
  - **OpenCA Labs**
  - **OpenCA PKI support for PRQP build in v1.1.0+**
  - **UNIX operating system(s)**
  - **Based on LibPKI library**
    - Ease-to-use PKI Library
- New release available (v0.5.0)
- Client implemented (?) in PKIF

# Conclusions

---

- Move PRQP from Experimental to Standard Track
  - **Move to standard-track I-D**
- Extend support for major clients
  - **Firefox**
  - **Operating Systems**
- Continue the development of the PRQP Server
  - **OpenCA Labs**

# Questions & Contacts

---

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

