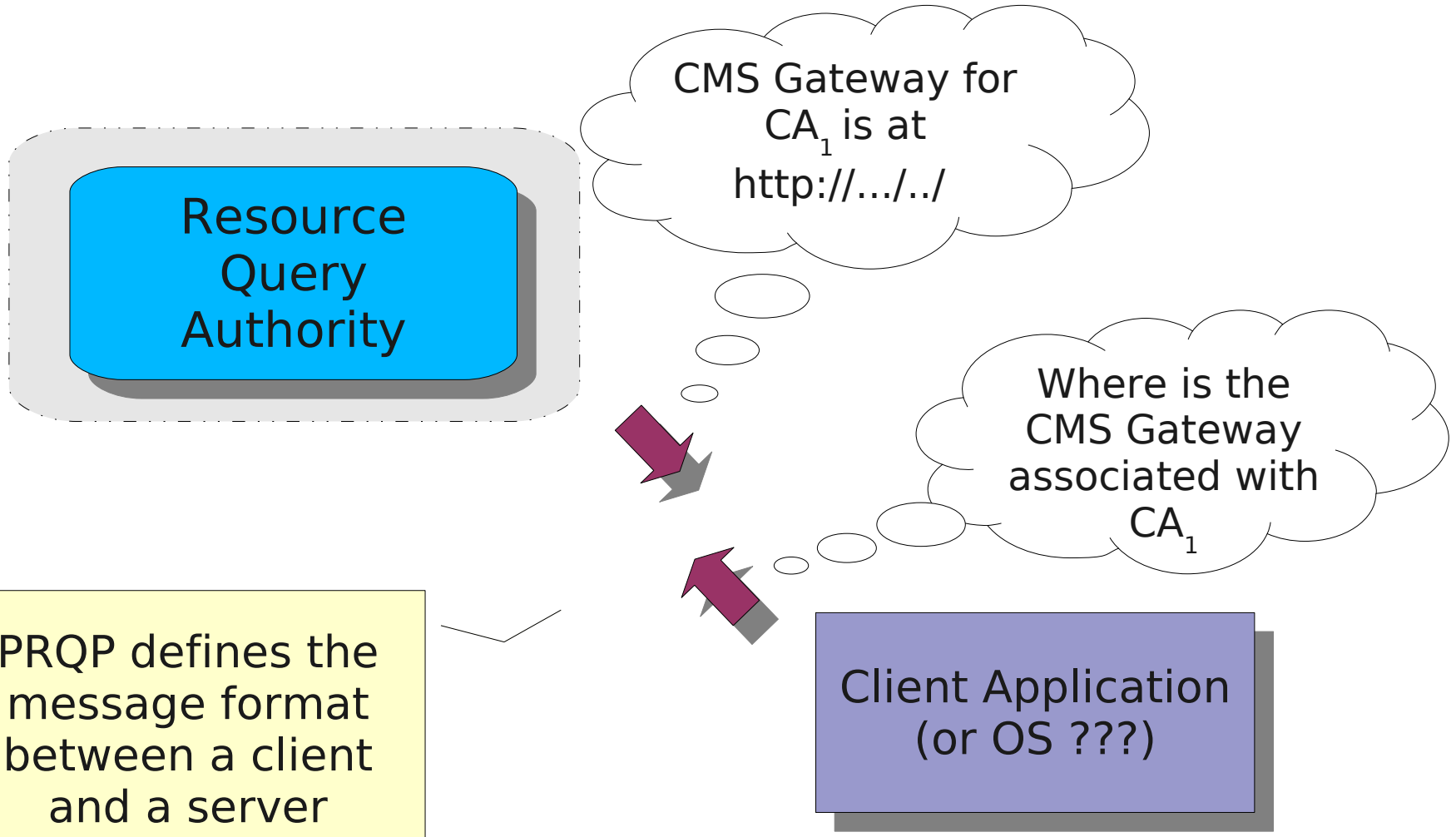
PKI Resources Query Protocol
Status Update & Recent Activities

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

PKI Resource Discovery Protocol



PRQP & Document Status

- Simple client-server protocol
- Defines two type of messages
  - **PRQP Request**
  - **PRQP Response**
- Available as individual contribution (should be moved to experimental, soon (?))
  - **I-D <draft-pala-prqp-01.txt>**
- Updated on Feb 2008
  - **Small changes in data structures (for response caching purposes)**
  - **Added OIDs to identify PKIX and Grid services**

Updated OIDs

	OID	Text	Description
PKIX	id-ad 1	ocsp	OCSP Service
	id-ad 2	calssuers	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

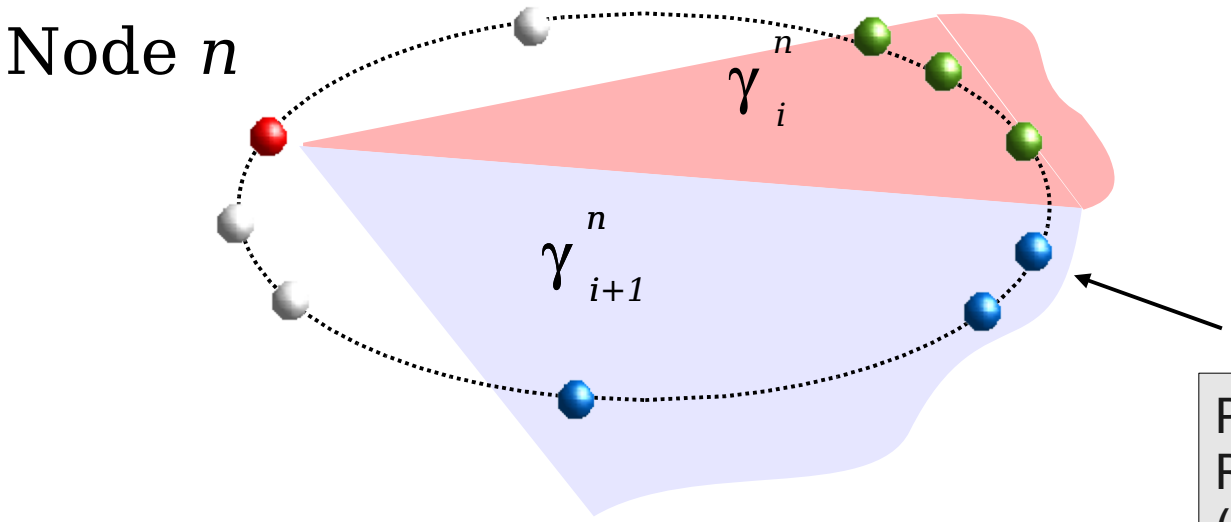
PRQP is enough ?

- Finding resources to PKI resources is crucial
- PRQP works in controlled environments
  - **Enterprises**
  - **Universities / Colleges**
- Interoperability
  - **We need an easy-to-deploy Discovery System**
- Current Activities:
  - **Definition of PEACH routing protocol (DHT)**
  - **PEACH enabled system**
    - PRQP-based Discovery System for PKI

PEACH Activities

- Definition of a Protocol for PRQP deployment over P2P network
  - **Peach**
- Distributed Hash Table
- Specifically targeted for PRQP
  - **Makes use of unique features from PRQP**
- Soon to be published as individual RFC

PEACH – A Discovery System for PKI (P2P Network of RQAs)



Participating Nodes are Resource Query Authorities (RQAs)

Peach Network provides a ***discovery system*** for all the participating CAs: the nodes are the RQAs

Conclusions

- Move PRQP to Experimental Status
- Submit draft about PEACH
- Start Discussion about PRQP & PEACH
- Study interactions with other PKIX work (e.g., TAM, SCVP, etc.)

Questions & Contacts

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