

\* = iPKI is not related to any Apple™ products, but the initial “i” is kinda cool

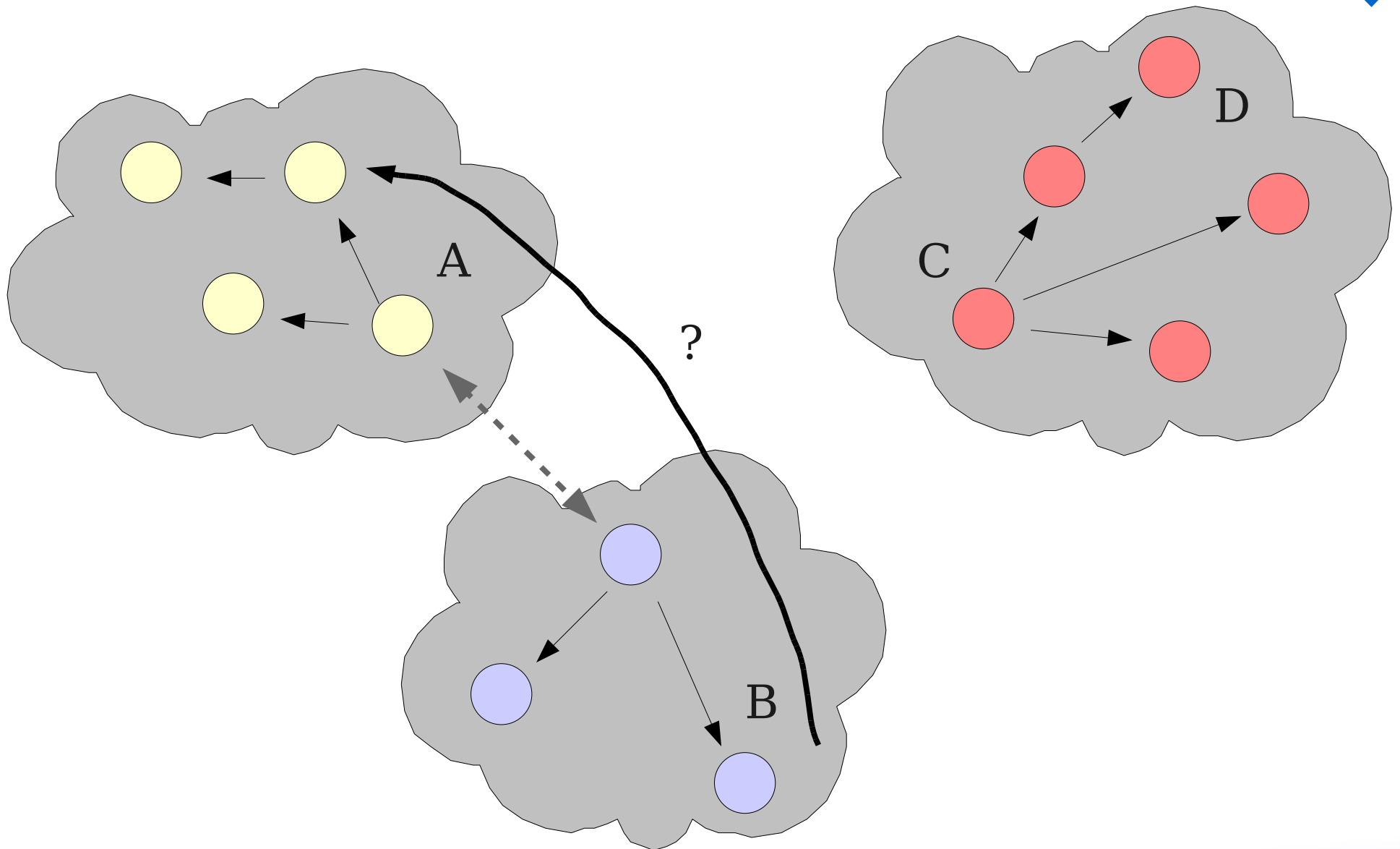
---

## **iPKI\* Updates: OpenCA, OpenCA-NG and PKI Discovery System**

... or shall we make PKIs *WORK*?

Massimiliano Pala  
<project.manager@openca.org>

# Path vs Resources Discovery



# Simple Questions

---

- Where do I apply for a new Certificate from this CA ?
- Where do I apply for my Certificate Renewal by using CMS ?
- Where do I apply to get my Certificate revoked ?
- Where do I find the Certificates repository ?
- Where do I download the CP/CPS ?
- Where do I find the SCVP from `this` CA ?
- What services are provided by my CA now ?

# Yes, We need a Solution!

---

- Finding resources to PKI resources is crucial
- Applications can provide simpler User Interfaces for users
  - ease configuration options
  - can take high-level trust decisions based on the level of security offered by available services or personal knowledge
- In some cross-organizations environments (Grids) even the distribution of simple CA information is a difficult task
- Everybody is doing things differently: we need to work on the matter and provide a specific (standardized) solution

# What is PRQP (so far...)

---

- Simple client-server protocol
- Defines two type of messages
  - PRQP Request
  - PRQP Response
- Available as individual contribution
  - I-D <pala-prqp-00.txt>
- Updates will be available soon (January)
- Small changes in data structures (for response caching purposes)

# What PRQP is not (so far...)

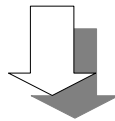
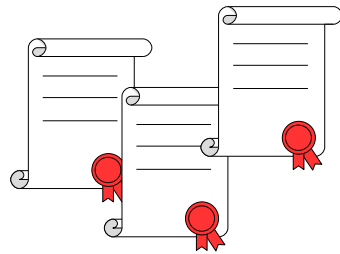
---

- A discovery System
- A data distribution System
- A validation Service (e.g., SCVP...)

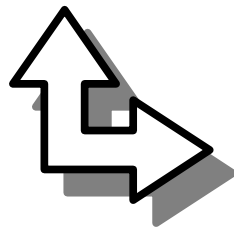
But it can be used to get pointers to such services from a trusted authority!

# Discovery System for PKI (Apps)

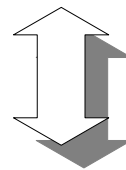
CA  
Certificates



Application

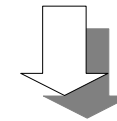
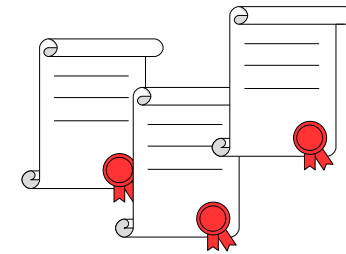


Services

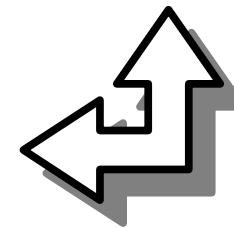


Resource  
Query  
Authority

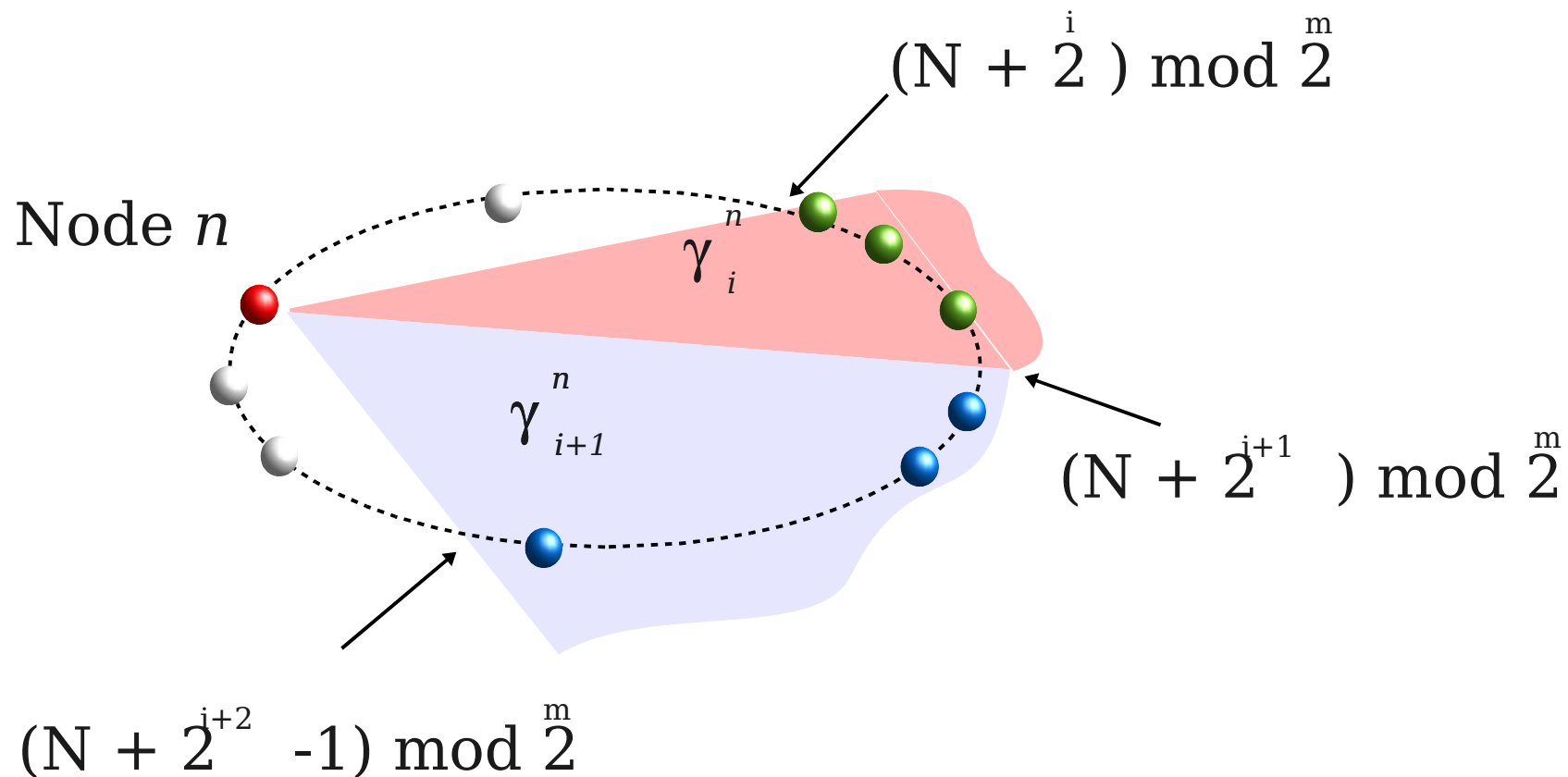
User  
Certificate(s)



Application



# Discovery System for PKI (P2P Network of RQAs)



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

# Currently Defined OIDs (draft-pala-prqp-01.txt)

	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

# Project Idea

---

- OpenCA-NG Design Principles:
  - Portable across different platforms
  - Full-featured
  - Easy-to-use
  - Pluggable Services
- Stand-alone Daemon (Written in C)
- Based on LibPKI
- Include Support for PKI Resource Discovery System
  - Query Protocol (PRQP)
  - Peer-2-Peer PRQP extension

# LibPKI

---

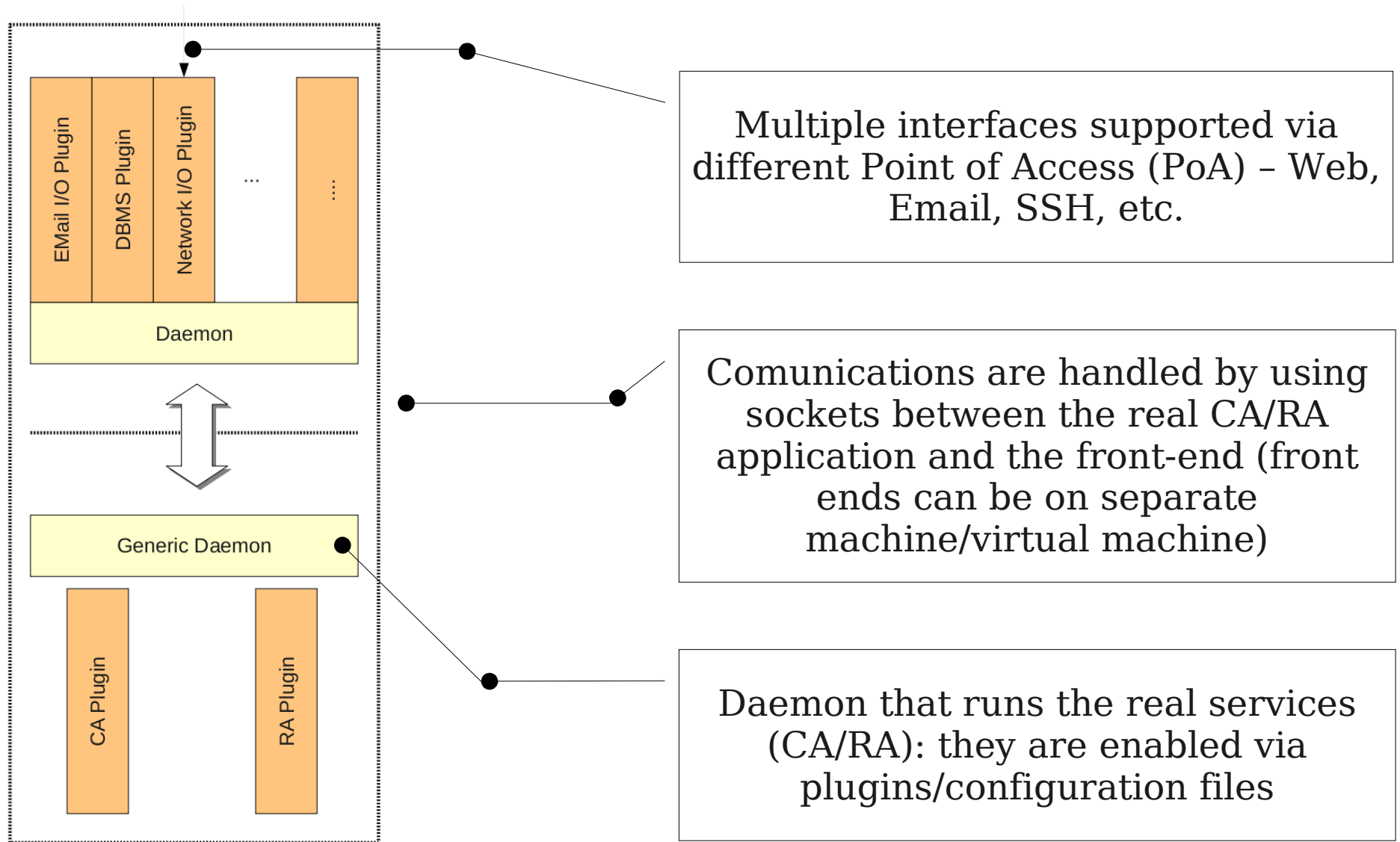
- LibPKI provides developers with an **easy-to-use high level API**
- Supports
  - X509v3 Certificates Handling
  - PKI Services (and Network data retrieval)
    - OCSP, CRLs, etc...
    - LDAP, HTTP, etc...
  - Hardware Devices
    - PKCS#11, OpenSSL ENGINE, KMF, etc...
  - Multiple Cryptographic Providers
    - OpenSSL, KMF, etc...

# LibPKI

---

- Supports (cont.)
  - XML configuration files handling
  - Certificate Stores
    - RDBMS, LDAP, etc...

# OpenCA-NG Design



# OpenCA & OpenCA-NG

---

- No timeline (!!!)
- No Project funding (anyone ???)
- Interests expressed by the industry
  - (but no formal commitment, yet)
- Reasonably starting in the summer
- OpenCA (1.0) release – next month
  - Security fix
  - Support for Vista

# Questions (???)

---



## **DISCLAIMER:**

No answer are guaranteed to be either intelligent nor appropriate. If you can read this, you are probably too close to the screen or you are simply cheating. Have a nice day.