Extending PKI Interoperability in Computational Grids

Scott Rea, Massimiliano Pala, Shreyas Cholia, and Sean Smith

Security, Trust and Privacy in Grid Environments Workshop

IEEE CCGrid, May 22 2008, Lyon, France

Outline

- Introduction
  - Introduction & Motivations
  - Current Solutions & Limitations
- PKI Data distribution and Trust Model
  - IGTF Trust Model
  - PKI Resource Query Protocol
- Conclusions
  - Implementation Details
  - Future Work

Introduction

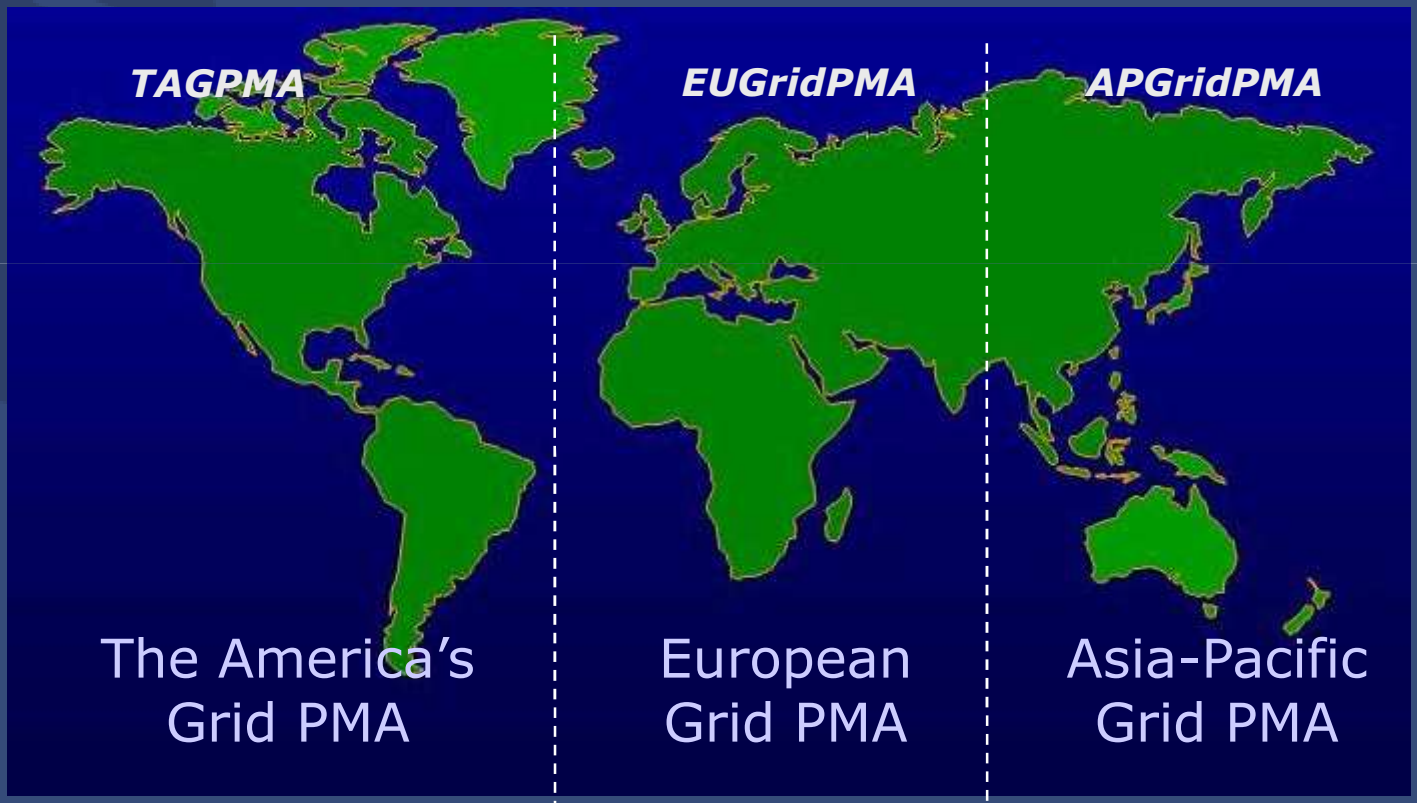
- Computational grids rely heavily on Public Key Infrastructures
  - Authentication in grids is PKI based
  - Authorization in grids can also be PKI based via VOMS
- The trust and integrity of grid transactions is underpinned by the PKIs that facilitate them
- Trust in any system that uses PKI can be defined by the following questions:
  - How well do I trust the issuer of a given credential to authenticate the identity of the subject of the credential?
  - How well do I trust the issuer of a given credential to bind the identity of the subject to the credential?
  - How well do I trust the subject to use the credential responsibly?

Introduction

- If there was a single PKI for all grid computing, evaluation of the issuer practices would be simple
- The International Grid Trust Federation helps to solve the evaluation of issuer practices for trusting many PKIs
  - 3-member PMA federation covering different regions of the world
  - Publish standard profiles on how Certificate Authorities should operate and issue credentials
  - Evaluate CAs policies and procedures against the profiles via peer review
  - Publish an official list of accredited CAs
  - Package trust anchors and relevant data for distribution

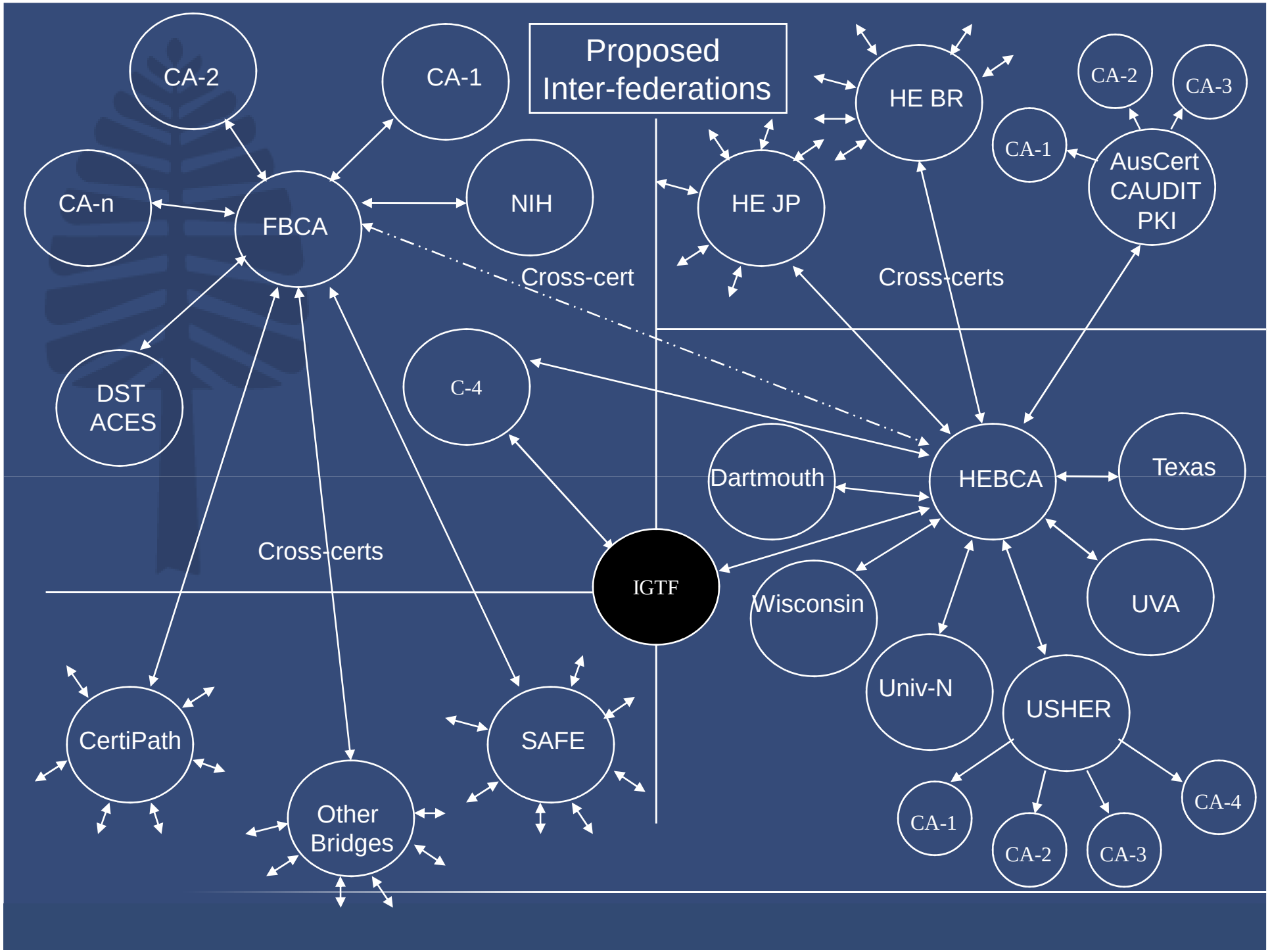
IGTF – the International Grid Trust Federation

- Common, global best practices for trust establishment
- Better manageability and response of the PMAs



Introduction

- Many grids also accept additional “local” PKIs for authentication and authorization purposes, that are not accredited by the IGTF
- The number of potential PKIs available to grids for authentication purposes is rapidly increasing
- Any grid that wants to take advantage of the plethora of PKIs available should carefully consider the policies and practices they employ to issue certificates
- The pressure for multiple sources of trusted PKIs and information regarding these PKIs is ever increasing
- Even if the IGTF accredited all these, the distribution would become to unwieldy for grids to process
- In future, grids will need a way to manage the subset of IGTF trust anchors that they wish to support and any additional “local” ones they also wish to trust


Proposed
Inter-federations
CA-2
CA-1
CA-n
FBCA
NIH
Cross-cert
DST
ACES
C-4
Cross-certs
IGTF
CertiPath
SAFE
Other
Bridges
HE BR
HE JP
CA-2
CA-3
CA-1
AusCert
CAUDIT
PKI
Cross-certs
Dartmouth
HEBCA
Texas
Wisconsin
UVA
Univ-N
USHER
CA-1
CA-2
CA-3
CA-4

Grids and PKI Data Distribution

- Download of trusted CA distributions
  - CA Certificates
  - CRL URL
  - Namespace
  - Signing Policy
  - *.info* (general information about the CA
- Possible Denial of Service
  - CRL downloaded at the same time by the Grid software
- Dynamic vs centralized Pull PKI data distribution model

Finding PKI Resources

- PRQP is a protocol that will allow relying parties to discover many different types of information about a given PKI
  - Validation Services (OCSP, SCVP, etc..)
  - Subscription/Revocation Services
- PRQP helps managing trusted PKIs details
- PRQP facilitates extended PKI interoperability within computational grids
  - Authorization framework
  - Attribute Authorities

Difficult PKI Questions (?)

Where can I ask for a certificate revocation ?

Where do I apply for a new Certificate ?

Where do I find the Certificates repository ?

PKI Resource Discovery

- Enhance Interoperability across PKIs
- Ease PKI Management Issues
  - Now connected to certificates' contents
- Foster simpler User Interfaces (UI)
  - User awareness Issues
- Usability of PKIs

Current Solutions

- Certificate Extensions
- DNS Records
- Web Services
- Local Network Oriented Solutions

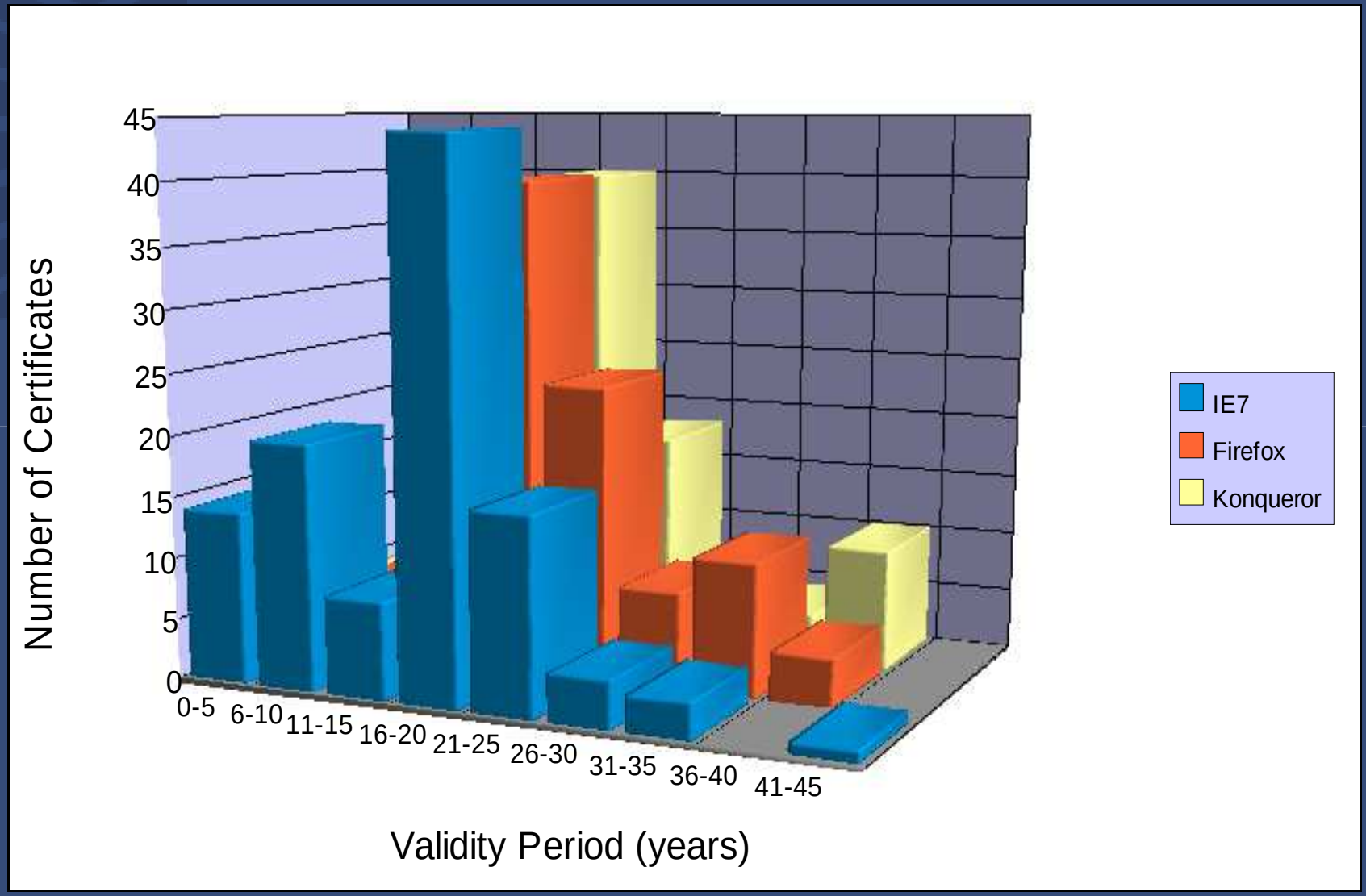
Certificate Extensions

- Certificate Extensions may be used to point to data and resources
  - AuthorityInformationAccess (AIA)
  - SubjectInformationAccess (SIA)
- *Different extensions for different locators (CDP, AIA/SIA)*
- *Too Static Approach*

Certificate Extensions

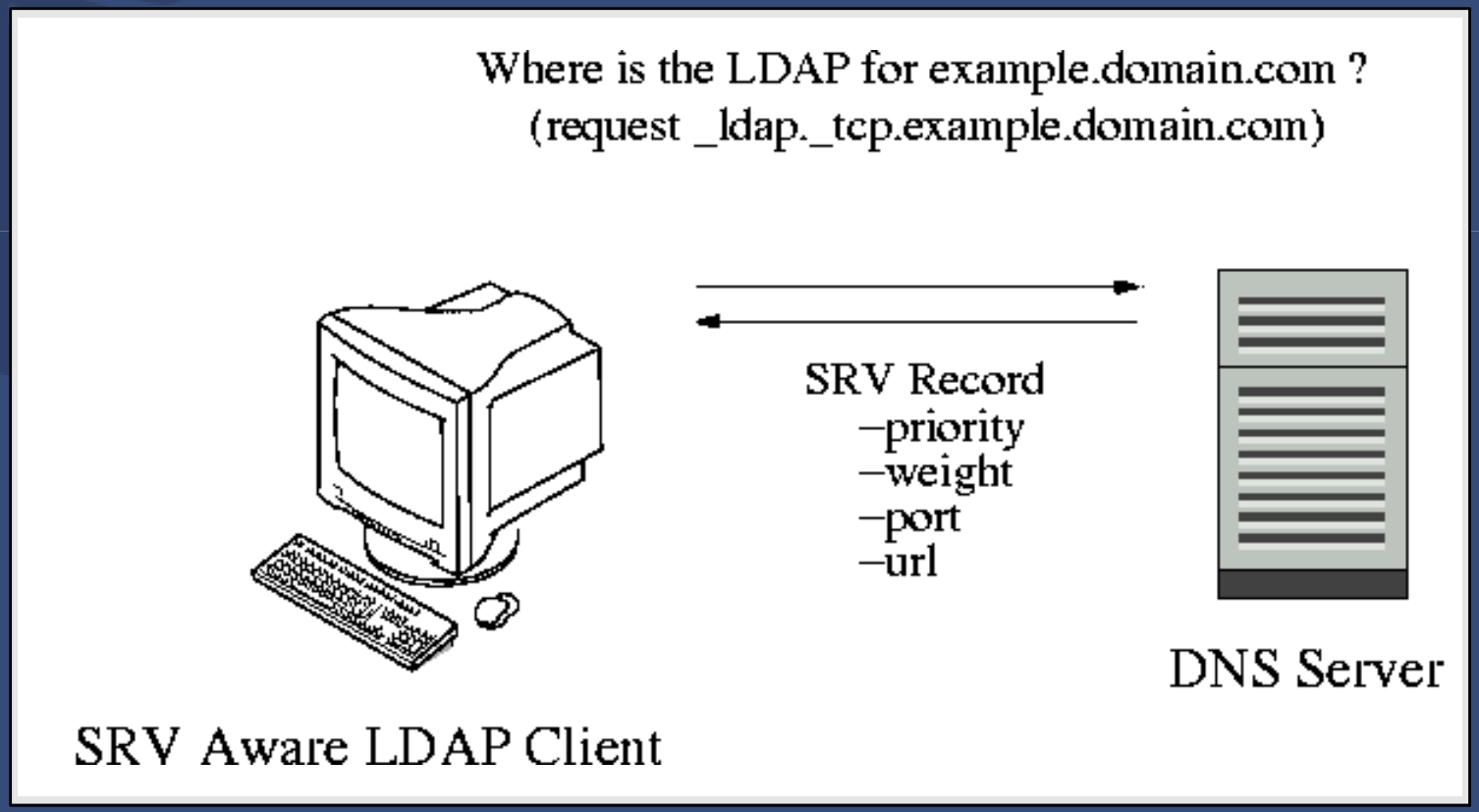
- Reissuing of certificates is needed for new extension values to be added/removed
  - feasible for CA's certificates
- Today
  - *OCSP pointer in 11% of Firefox Embedded Certs*
  - *No pointers in IE/KDE applications*

Certificate Extensions



DNS Records

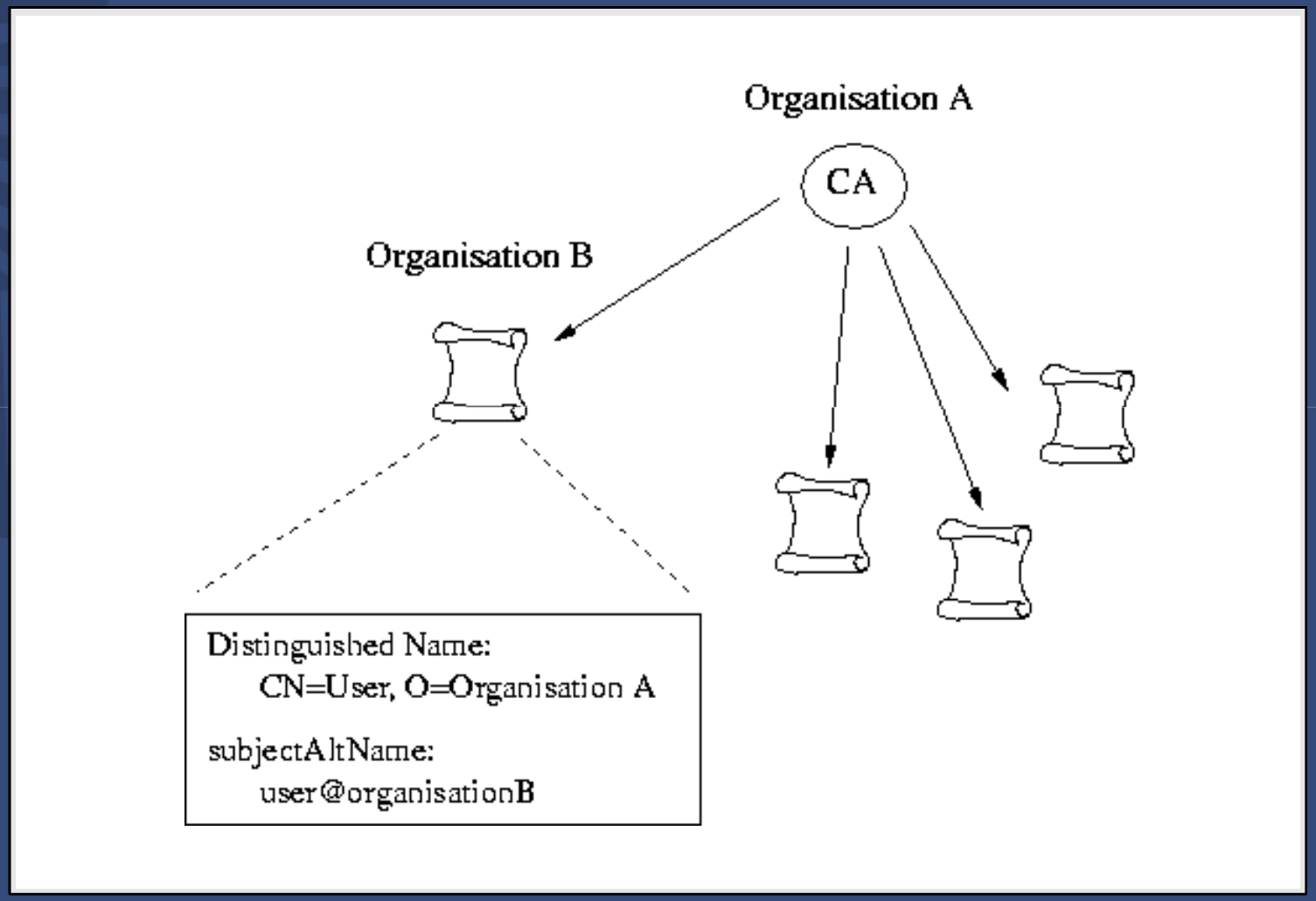
- DNS SRV Records can be used to store informations about provided services
- Provides pointers to servers in a certain domain



DNS Records: Open Issues

- Name space mapping issues
  - X500 global namespace never made it (sorry David)
  - No relationship between DNS names and PKI's Name Spaces (unless DC=”” format is used)
- The issuing organization does not always have control over DNS records
- Where domain should the client query?

DNS Records: Open Issues (cont.)



Webservices

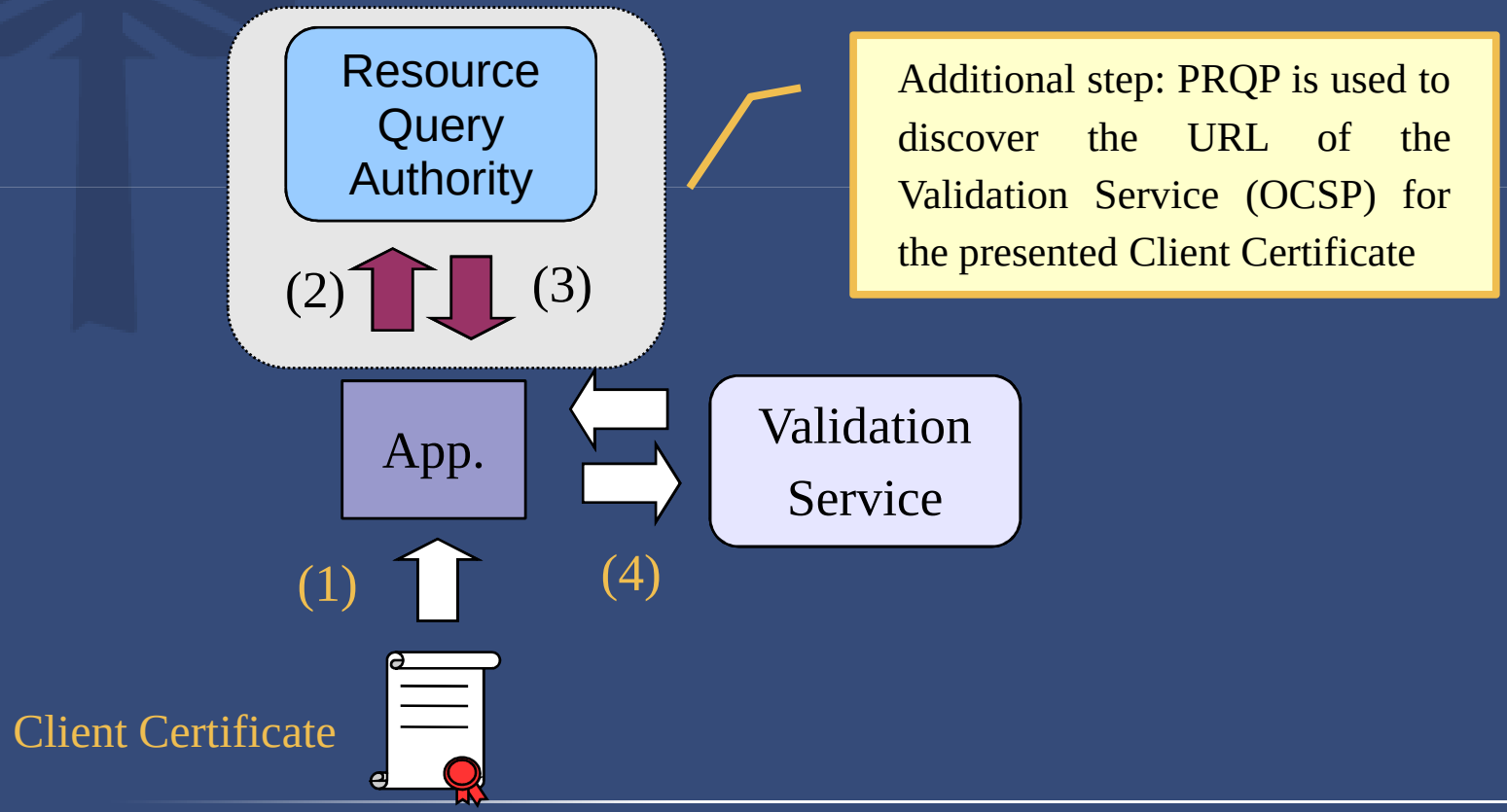
- applications can discover available webservices (by using SOAP, WSDL and UDDI)
- Easier than CORBA.. but...
- Issues:
  - Complex to deliver (WSDL, SOAP, UDDI)
  - Verbose XML format
    - cumbersome for mobile devices
  - XML not really supported by every X509 clients
    - Schemas (?!?!?)

The Proposed Solution

- The PKI Resources Query Protocol
- Allows a client to request services and repositories URL associated with a CA
- Provides “discovery” for any services (current and future):
  - Repositories (CRLs and Certs)
  - Validation Services (OCSP, SCVP, etc...)
  - Other Services (TimeStamping, Revocation, Subscription, etc...)
  - Future services

The Request Query Authority

- Authority designated to answer to PKI Resource Location
- Provides pointers to resources related to a CA



Implementation Details

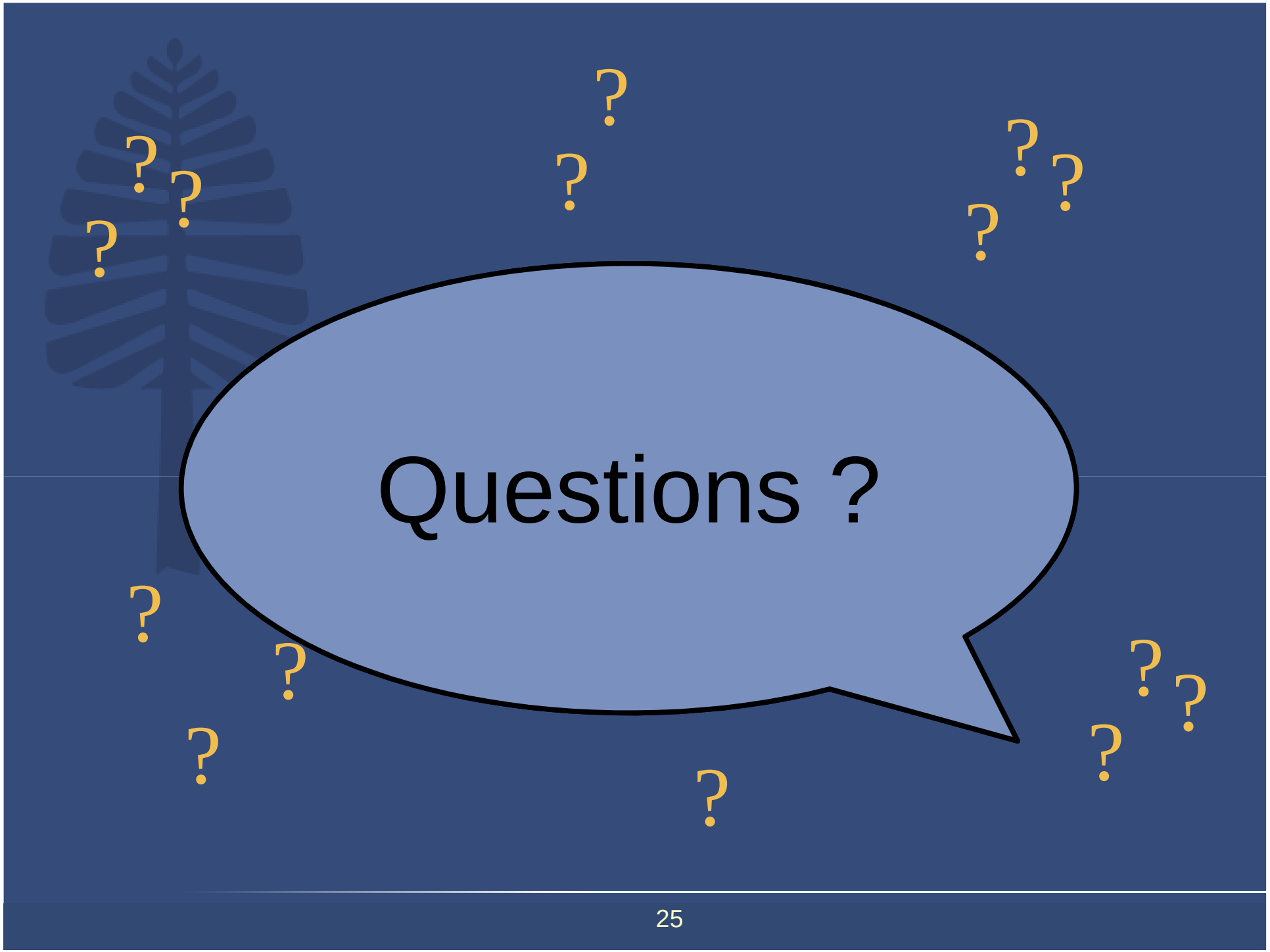
- PRQP API included into LibPKI (v0.1.8)
  - Provides easy-to-use functionality
    - PRQP_REQUEST_new_cert_file()
    - PRQP_REQUEST_new_cacert_file()
- CLI Utility (command line)
  - Generates a PRQP requests
  - Sends it to a specified RQA via HTTP
  - Prints out the PRQP response
- PRQP Server (available version at OpenCA - v0.1.1)
  - Based on OpenCA OCSPD
  - Implements PRQP over HTTP

Conclusions

- Dynamic Solution
- Fast and easy to implement
- Specific solution for the problem
- Ease rollover of services
- Facilitates extending PKI interoperability within Grids
  - Ease integration of new Trust Anchors
- PKI usability
  - Ease PKI management
  - less client/server configurations needed
- Dynamic PKI Data distribution model
  - More scalable than Centralized Pull model

Future Works

- PKI ***Usability and Interoperability project*** at Dartmouth College:
  - Advance the IETF Proposal (pala-prqp-01.txt) as new Working Item for PKIX-WG (now on experimental track)
  - Study and Deploy an RQA (Resource Query Authority)
    - Guys, we need your CAs' data
  - Extending the PRQP to a Peer-2-Peer Authenticated Network (PEACH Network)
    - Work will be presented at EuroPKI 2008


Questions ?

Thank You!

- Contacts:

Massimiliano Pala <pala@cs.dartmouth.edu>

OpenCA <project.manager@openca.org>

Scott Rea <Scott.Rea@dartmouth.edu>

HEBCA <HEBCA@Dartmouth.EDU>

- Website

https://www.openca.org/projects/prqpd/