Using OGRO to implement OCSP Certificate Validation in the Globus Toolkit 4

Jesús Luna
Oscar Manso
Manel Medina

Polytechnical University of Catalonia
Computer Architecture Department
Barcelona, Spain

Agenda

- Motivation
- OCSP Requirements for Grids
- CertiVeR and OGRO: an OCSP infrastructure for Grids
- OCSP Prevalidation and second-Level Caching
- Conclusions and Future work

Motivation

- Cryptographic credentials in the form of X.509 Certificates are widely used into the Grid:
  - Proxy Certificates (delegation), Service's startup, Job Management, etc.
- Moreover, they are the cornerstones for Authentication and Authorization processes.
  - Must be Authenticated: private key, digital signature, validity period, Trust Anchors.
  - And Authorized: roles, attributes, group membership, policies.
- But...What if a Certificate has been compromised? How can I propagate the revocation information through the VO?

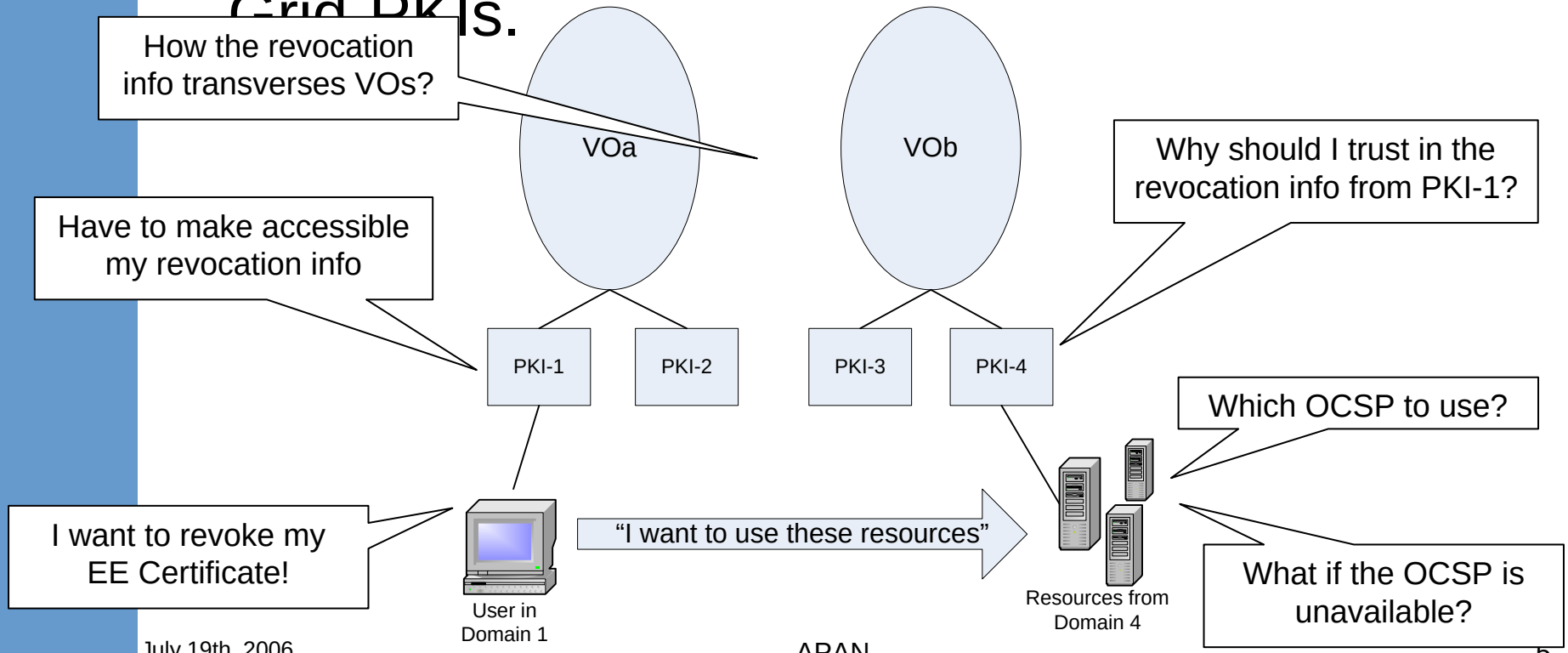
Motivation (2)

- CRL (RFC 3280):
  - Historically used in Grids.
  - Cumbersome solution: i.e. very large Grid's CRLs.
  - No fault tolerance.
  - No real-time solution.
- OCSP (RFC 2560):
  - Complement Grid CRLs.
  - Based on a Request-Response protocol, suitable for Grids.
  - Still no fault tolerant.
  - Almost real-time.

And we still need to consider some "special" validation requirements for Grids!

OCSP Requirements for Grids

- Requirements currently being drafted at GGF's CA Operations Workgroup. Almost there!
- Multiple VOs, each one can support several Grid PKIs.



In summary

- So far at the CAOPS-WG identified the following OCSP requirements for Grids:
  - Network Transport: HTTP/HTTPS.
  - Revocation sources: CRL, OCSP, DB…
  - Responder Discovery: AIA, Server list…
  - High performance and fault tolerant OCSP Responders.
  - OCSP Server's Signing keys: trusted responder, authorized responder or transponder.
  - Others: use of nonce, digital signatures, caches…

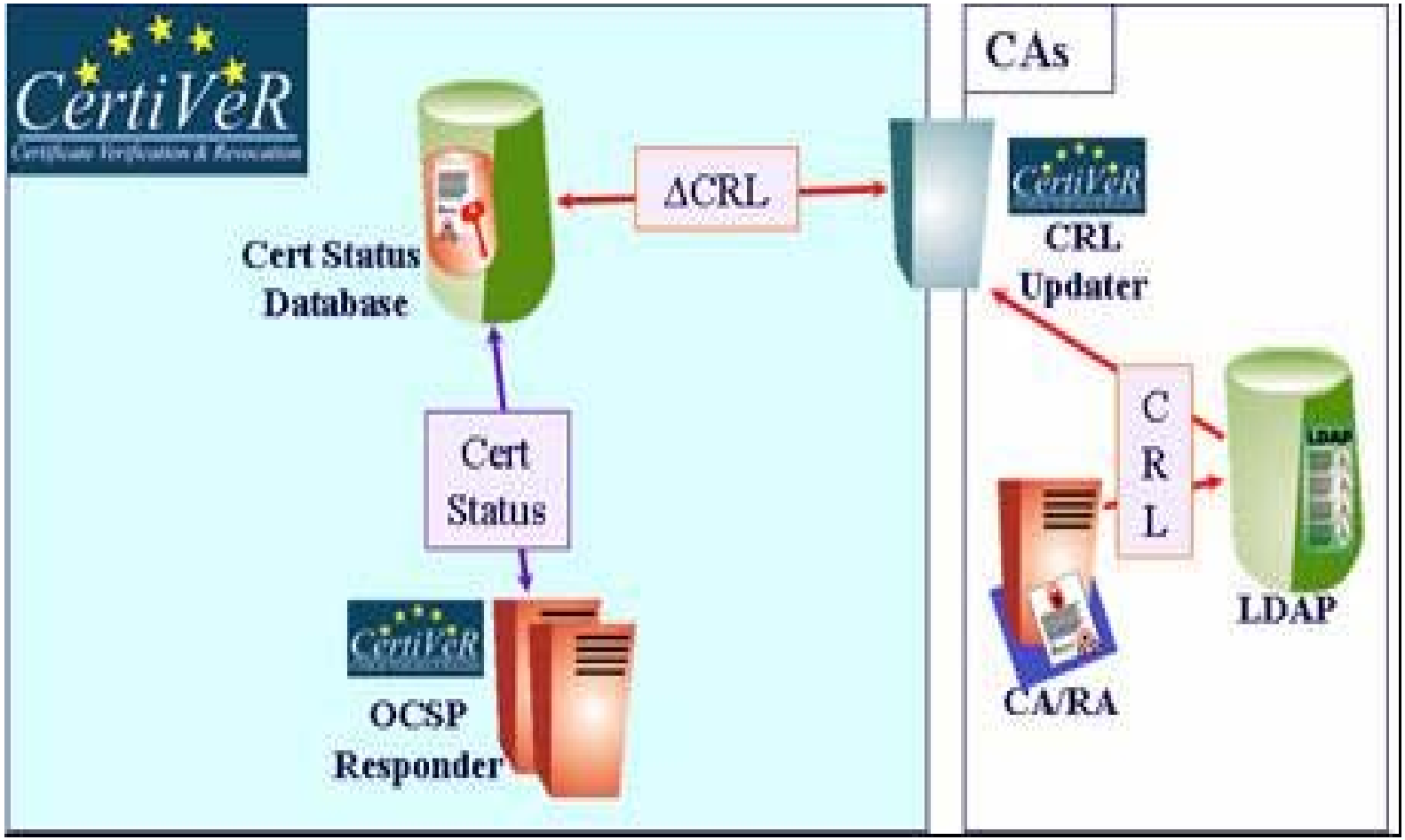
CertiVeR and OGRO: an OCSP infrastructure for Grids

CertiVeR
Certificate Verification & Revocation

CertiVeR

- UE Funded project.
- Distributed architecture.
- May work as Trusted, Authorized or Clearinghouse Responder.
- Able to parse customized OCSP Response Extensions (i.e. CA's trust degree).
- Supports Proxy Certificate Validation.
- Fault Tolerant.

CertiVeR's Architecture



OGRO
(Open GRid Ocsp)

- Grid-OCSP Client for the Globus Toolkit 4.
- Open Source, 100% Java.
- Not reinventing the wheel: Developed over well-known JCE Providers (BouncyCastle and soon IAIK/J2SE5).
- Implements GGF's Relying Party recommendations.
- Easily configurable through the *Grid Validation Policy –GVP-*.

Grid Validation Policy

- Set of XML rules to customize OCSP validation behavior per-Issuer:
  - Revocation Sources discovery and querying,
  - Error Handlers,
  - OCSP Request/Response tailoring,
  - Unknown status treatment,
  - Proxy Certificate's validation.

GVP Example

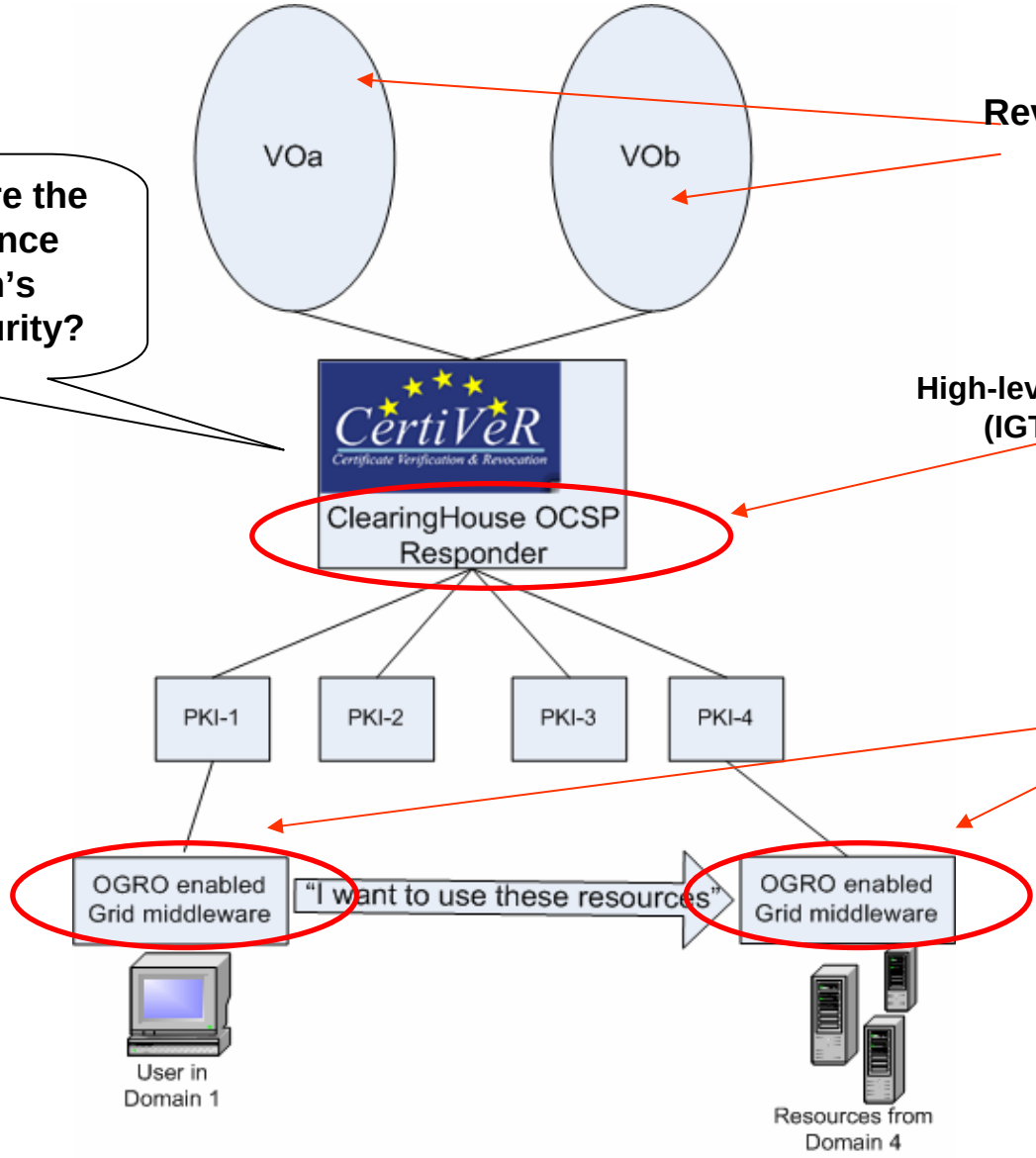
```
<?xml version="1.0"?>
<!DOCTYPE ocsppolicy SYSTEM "ocsppolicy.dtd">
<ocsppolicy>
  <issuerdn dn="C=ES,O=CertiVeR,2.5.4.45=2003,CN=AC CertiVeR"
            name="AC CertiVeR" hash="o6MjoB5y4b2cNvILPcBxWafHs7k=" >
    <unknownstatus action="revoked" />
    <errorhandler>
      <action order="1" type="tryLater" maxRetries="2" />
      <action order="2" type="setFinalResponse" value="revoked" />
    </errorhandler>
    <request>
      <signrequest value="true" />
      <usenonce value="true" />
      <protocol value="https" />
     <extension order="1" value="CA_RATING_EXTENSION"
        oid=" 1.3.6.1.4.1.4710.2.454.10.1.1 " />
    </request>
  </issuerdn>
  <issuerdn name="default" dn="*" hash="na" >
    <revsources>
      <source order="1" location="http://tacar.certiver.com"
        timeout="3600" type="trusted" />
      <source order="2" location="http://globus-grid.certiver.com"
        timeout="3600" type="trusted" />
    </revsources>
    <proxycert>
      <unknownstatus action="good" />
    </proxycert>
  </issuerdn>
</ocsppolicy>
```

Comparing OGRO

Grid-OCSP Requirement	J2SE5	Bouncy Castle	IAIK	OpenSSL client	Ascertia OCSP Client	OGRO
Transport HTTP/HTTPS	Both	Both	Both	Both	Both	Both
Revocation Source Requirements	AIA, OCSP, CRL	No	No	CRL/OCSP	AIA, OCSP. Keeps list of Trusted Responders	AIA, OCSP, CRL. Query order in Grid Val Policy (GVP).
Use of nonce	Not specified	Yes	Yes	Yes	Yes	Yes
Error Handlers	First AIA, if not present OCSP. Fallback to CRL.	No	No	Cautionary Period-like mechanism	No	Query whole GVP's Rev. source list N-times. Set final status if failed.
Unknown Status Management	No	No	No	No	No	Yes
OCSP Request Signing	Not specified	Yes	Yes	Yes	Yes	Yes
Flexible Configuration	Some default parameters configured into JCE.	No	No	Configura-tion File for default params.	GUI configurator for default parameters.	Flexible ruleset with GVP.

Proposed Grid Validation Infrastructure

BUT…How to configure the GVP to obtain a balance between Validation's performance and security?



OCSP Prevalidation and Second-Level Caching

- Several configurations of the GVP were tested, by combining different parameters (transport protocol, nonce, sign request, etc.).
- We found that overall OCSP overhead was pretty similar in all the cases, but very high!
- A couple of performance enhancements have been introduced: prevalidation and second-level caching.

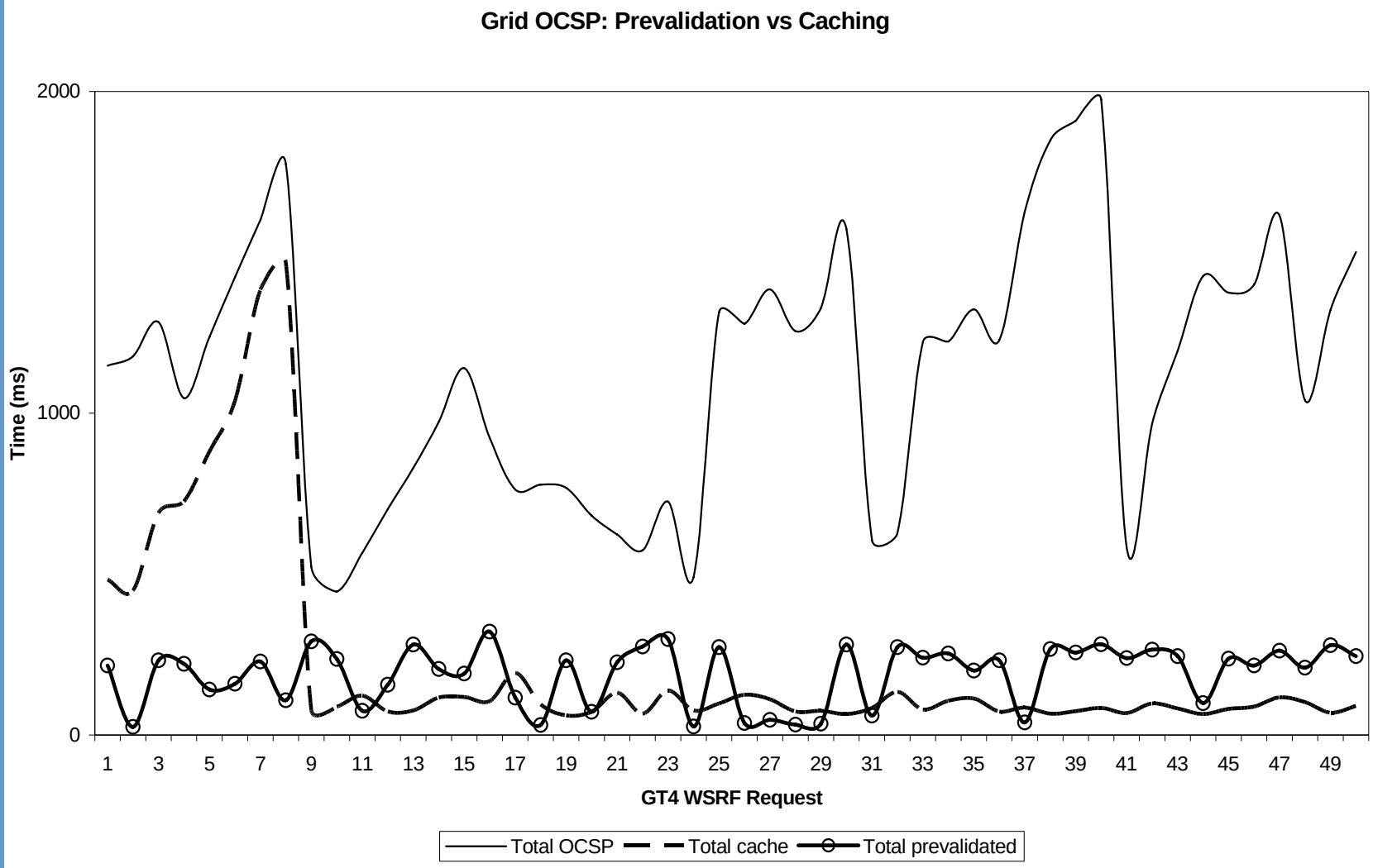
Prevalidation

- What if…:
  - Move OCSP overhead to Grid Clients, thus keeping Grid Server and OCSP Responder exchanges to a minimum.
- Prevalidation:
  - Embed the OCSP Response as a Proxy Certificate's X.509 extension. This is a fairly secure validation token (i.e. digitally signed and time-stamped)
  - When the Grid Server authenticates the Proxy certificate, will also validate it by extracting the prevalidation data.
  - Verify the prevalidation data to avoid potential security risks!

Second-Level Caching

- Hierarchical OCSP Caching recommended by CAOPS-WG: Grid client (first level), Grid Server (second level) and OCSP Responder (third level).
- Second-level caching:
  - Reduces communication between Grid server and OCSP Responder.
  - While “warming” will behave like *traditional* OCSP, but afterwards may be better than prevalidation.
  - Must control stale entries.
  - May provide a solution in case of OCSP Responder absence due to failures.

Results


Grid OCSP: Prevalidation vs Caching
Time (ms)
2000
1000
0
1
3
5
7
9
11
13
15
17
19
21
23
25
27
29
31
33
35
37
39
41
43
45
47
49
GT4 WSRF Request
Total OCSP
Total cache
Total prevalidated

Conclusions (1)

- OCSP is suitable for Grid environments but special requirements are introduced by its use.
- To gain practical experience we have developed an OCSP infrastructure:
  - CertiVeR.
  - OGRO.
- As far as we know there are no others Grid-OCSP implementations for the GT.

Conclusions (2)

- Performance issues:
  - Almost the same for different OCSP relying party's configurations.
  - Still too high for Grids expecting millions of validations (i.e. LHC).
- Prevalidation and Second-level caches introduced as performance enhancements.
- Much better performance and security features, so the choice will depend on VO's existing and new security requirements (i.e. Proxy Certificate's revocation).

Future work

- Validation performance is being greatly enhanced, expect new results soon!
  - Extending OCSP Response “lifetime”: cautionary period and new OCSP messages.
  - Hybrid approaches combining Prevalidation and Second-Level Caches.
- Working towards a Credential Validation System (GGF, DoE) by extending OGRO and CertiVeR:
  - Grid-PKI CP’s being evaluated and such data transported in the form of OCSP extensions (static validation).
  - Validation Policy being extended so it can be evaluated by the Grid Server when a request arrives, thus identifying appropriate set of resources (dynamic evaluation).

Gracias!

- Please test drive our OCSP Infrastructure with your Grids:

  http://www.certiver.com

  http://globus-grid.certiver.com/info/ogro

Questions?

jluna@ac.upc.edu
medina@ac.upc.edu
o.manso@certiver.com