EUROPEAN MIDDLEWARE INITIATIVE

Argus policies in action

Andrea Ceccanti (INFN)

On behalf of the Argus PT

What is authorization?

Can user X perform action Y on resource Z ?

Authorization examples

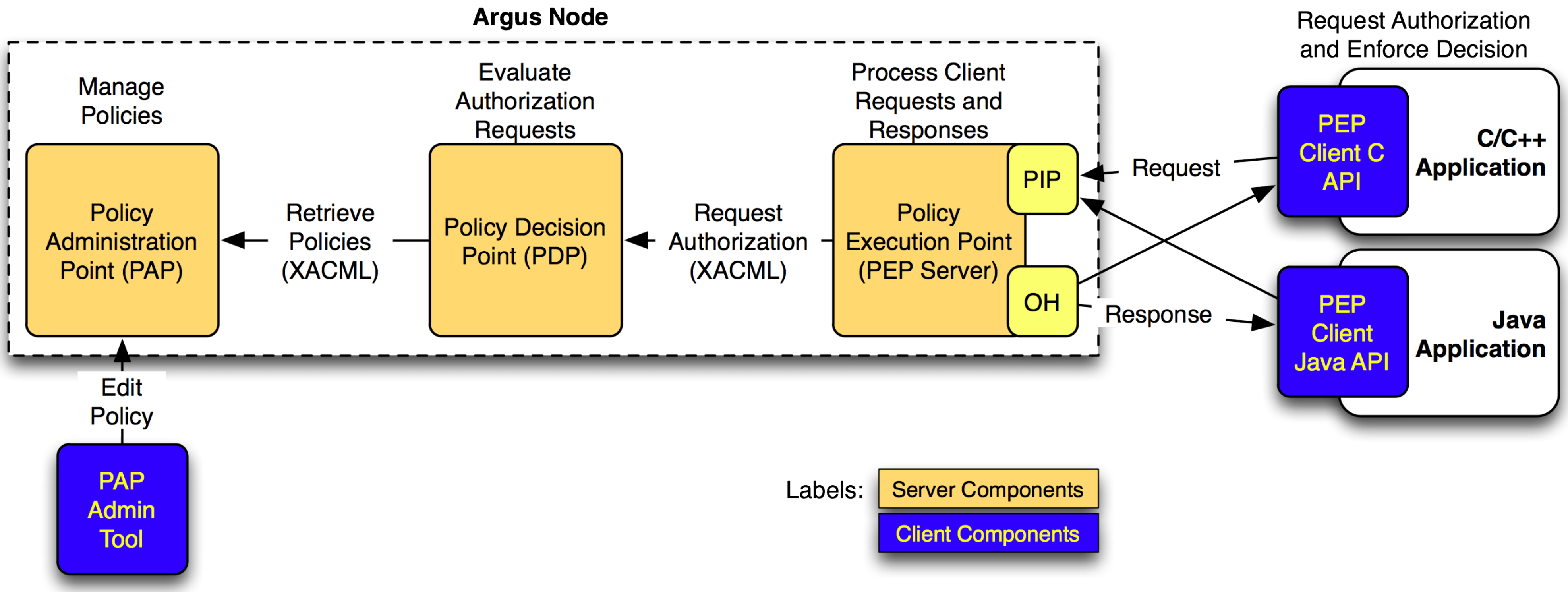
- Can user X
  - execute on this Worker node?
  - submit a job on this CREAM CE?
  - access this storage area?
  - submit a job on this WMS instance?

Motivations for Argus

- Each Grid service has its own authorization mechanism
  - Administrators need to know them all
  - Authorization rules at a site are difficoult to understand and manage
- No global banning mechanism
  - Urgent ban of malicious users cannot be easily and timely implemented on distributed sites
- Authorization policies are static
  - Hard to change policies without reconfiguring services
- Monitoring AuthZ decisions is hard

Argus

- A generic authorization system
  - Built on top of an XACML policy engine
  - renders consistent authorization decisions based on XACML policies



Argus Node
Manage Policies
Policy Administration Point (PAP)
Retrieve Policies (XACML)
Evaluate Authorization Requests
Policy Decision Point (PDP)
Request Authorization (XACML)
Process Client Requests and Responses
Policy Execution Point (PEP Server)
PIP
OH
Request
Response
Request Authorization and Enforce Decision
PEP Client C API
C/C++ Application
PEP Client Java API
Java Application
Edit Policy
PAP Admin Tool
Labels:
Server Components
Client Components

Argus components

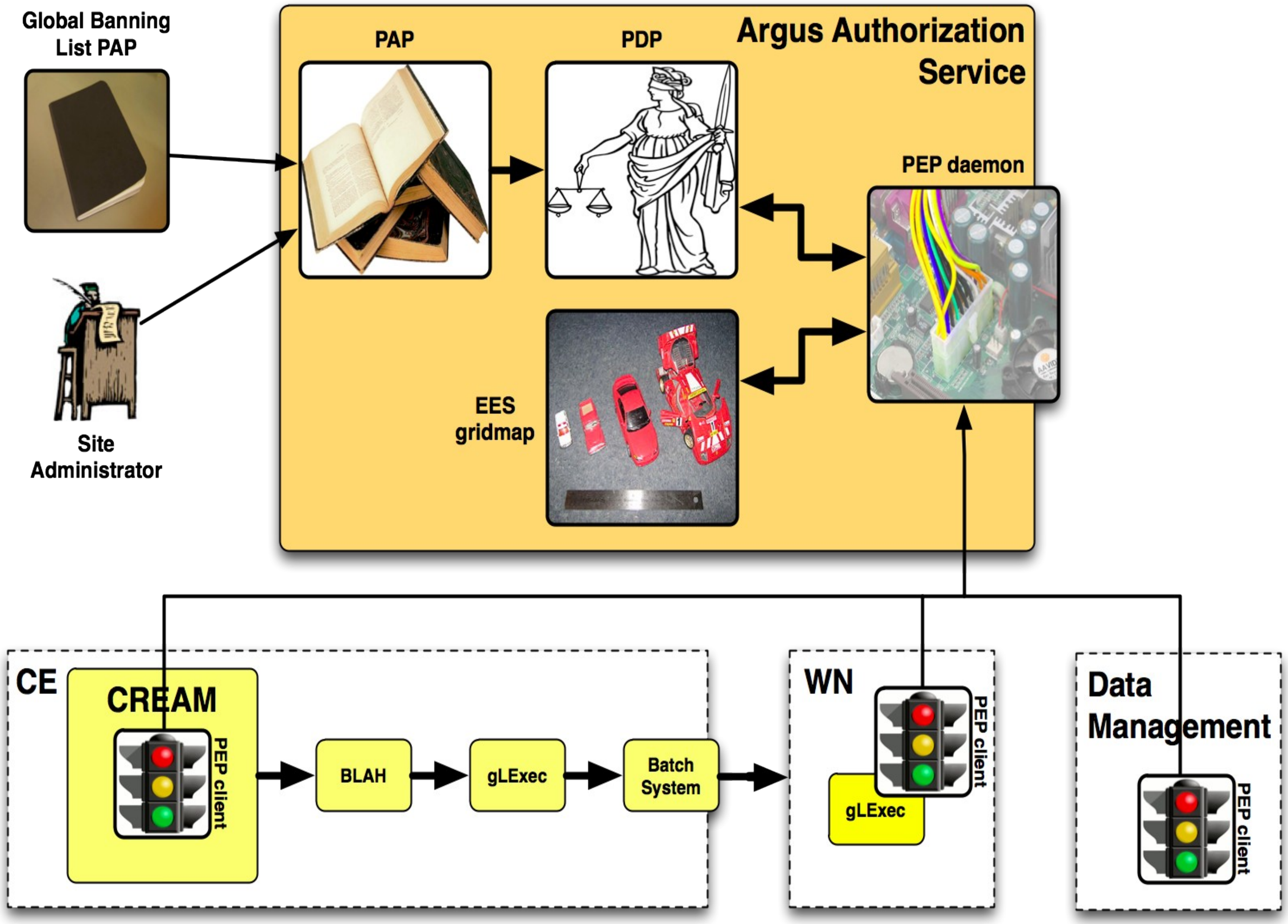
- **Policy Administration Point** (PAP)
  - Provides administrators with the tools to author policies
  - Stores and manages authored XACML policies
  - Provides managed authorization policies to other authorization service components (other PAPs or PDPs)

- **Policy Decision Point** (PDP)
  - Policy evaluation engine
  - Receives authorization requests from the PEP
  - Evaluates requests against policies fetched from the PAP
  - Renders the authorization decision

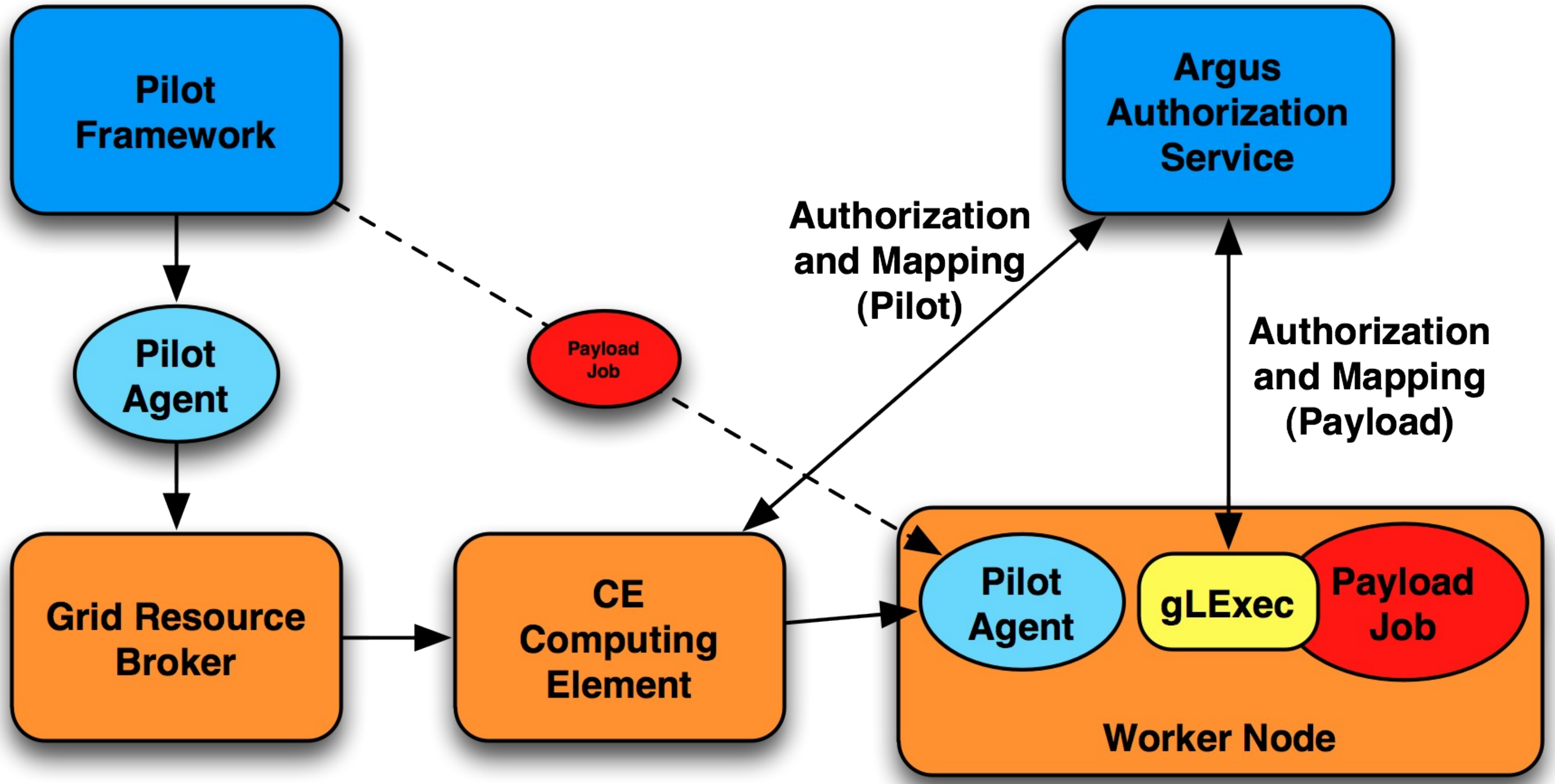
Argus components (cont.)

- **Policy Enforcement Point** (PEP)
  - Client/Server architecture
  - Lightweight PEP client libraries (C and Java)
  - PEP server receives the authorization requests from PEP clients
    - Transform lightweight internal request in XACML request
    - Applies a configurable set of filters (PIPs) to the incoming request
    - Asks the PDP to render an authorization decision
    - Applies Obligation Handler to determine user mapping, if requested by the PDP

Argus service deployment



Pilot job authorization



Argus policies

Argus is designed to answer the question:

Can user X perform action Y on resource Z?

Argus policies contain rules that state which actions can be performed on which resources by which users.

Argus uses XACML v.2.0 as the policy language.

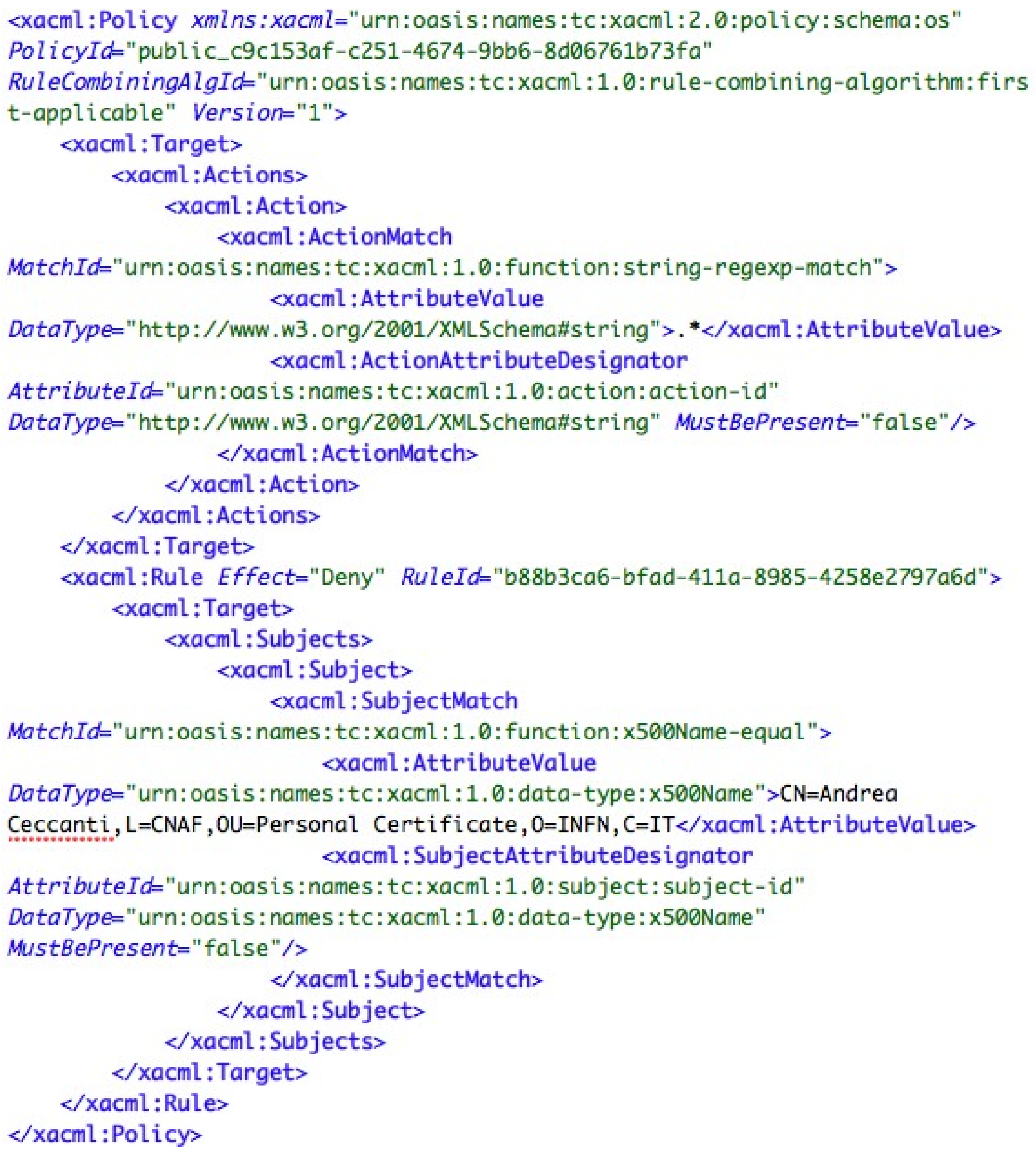
- however, XACML is hard to read and write, so we developed a **Simplified Policy Language (SPL)** to suit our needs

The banning use case

User X should not be allowed to do anything on any resource

(for this example X will be my certificate subject)

The XACML banning policy



```
<xacml:Policy xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
PolicyId="public_c9c153af-c251-4674-9bb6-8d06761b73fa"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:firs
t-applicable" Version="1">
    <xacml:Target>
        <xacml:Actions>
            <xacml:Action>
                <xacml:ActionMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">
                    <xacml:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">.*</xacml:AttributeValue>
                    <xacml:ActionAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="false"/>
                </xacml:ActionMatch>
            </xacml:Action>
        </xacml:Actions>
    </xacml:Target>
    <xacml:Rule Effect="Deny" RuleId="b88b3ca6-bfad-411a-8985-4258e2797a6d">
        <xacml:Target>
            <xacml:Subjects>
                <xacml:Subject>
                    <xacml:SubjectMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:x500Name-equal">
                        <xacml:AttributeValue
DataType="urn:oasis:names:tc:xacml:1.0:data-type:x500Name">CN=Andrea
Ceccanti,L=CNAF,OU=Personal Certificate,O=INFN,C=IT</xacml:AttributeValue>
                        <xacml:SubjectAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
DataType="urn:oasis:names:tc:xacml:1.0:data-type:x500Name"
MustBePresent="false"/>
                    </xacml:SubjectMatch>
                </xacml:Subject>
            </xacml:Subjects>
        </xacml:Target>
    </xacml:Rule>
</xacml:Policy>
```

... ?

The SPL policy

```
resource ".*" {
 action ".*" {
  rule deny {

   subject="CN=Andrea Ceccanti,L=CNAF,OU=Personal Certificate,O=INFN,C=IT"

  }
 }
}
```

Identifying Actions and Resources

- Actions and resources are identified by unique “names” that are assigned to them
  - Tipycally URIs, but any string will work

- Resource ID example:
  - http://authz.cnaf.infn.it/resource/cream-ce

- Action ID example:
  - http://authz.cnaf.infn.it/action/submit-job

Identifying subjects

A Subject in a policy can be identified via the following attributes:

- **subject**, an X509 certificate subject

```
subject="CN=Andrea Ceccanti,L=CNAF,OU=Personal Certificate,O=INFN,C=IT"
```

- **ca**, the CA certificate subject

```
ca="CN=INFN CA,O=INFN,C=IT"
```

- **vo**, the name of the Virtual Organization

```
vo="cms"
```

- **fqan**, a VOMS fully qualified attribute name

```
fqan="/atlas/production"
```

- **pfqan**, the VOMS primary FQAN

```
pfqan="/atlas/Role=pilot"
```

SPL Syntax

```
resource <value> {

    action <value> {

        rule <permit|deny> {

        <attributeId> = <attributeValue>

        }
        ...
    }
    ...
}
...
```

Order matters!

Obligations

```
obligation <obligationId> {
   <attributeId> = <attributeValue>
   ...
}
```

- Obligations define a set operations that must be performed by the Argus PEP in conjunction with an authorization decision
- Obligation stanzas can be defined in the resource or action context, and can contain attribute definitions

map-to-local-environment

- The map-to-local-environment obligation, identified by the id:
  - `http://glite.org/xacml/obligation/local-environment-map`
- is used within a policy to signify that a mapping to a local posix account will be produced by the Argus server as a result of a permit policy.
- The use of this obligation is **mandatory** for the policies that authorize the execution and mapping of jobs on the worker node and the CREAM CE

The pap-admin tool

- List currently active policies:
  - pap-admin list-policies
- Import policies expressed in SPL from a file:
  - pap-admin add-policies-from-file policies.txt
- Ban/Unban users:
  - pap-admin ban vo atlas
  - pap-admin unban vo atlas
- Add a generic permit/deny policies
  - pap-admin add-policy --resource “ce_1” --action “.*” \
    permit fqan=”/atlas/production”

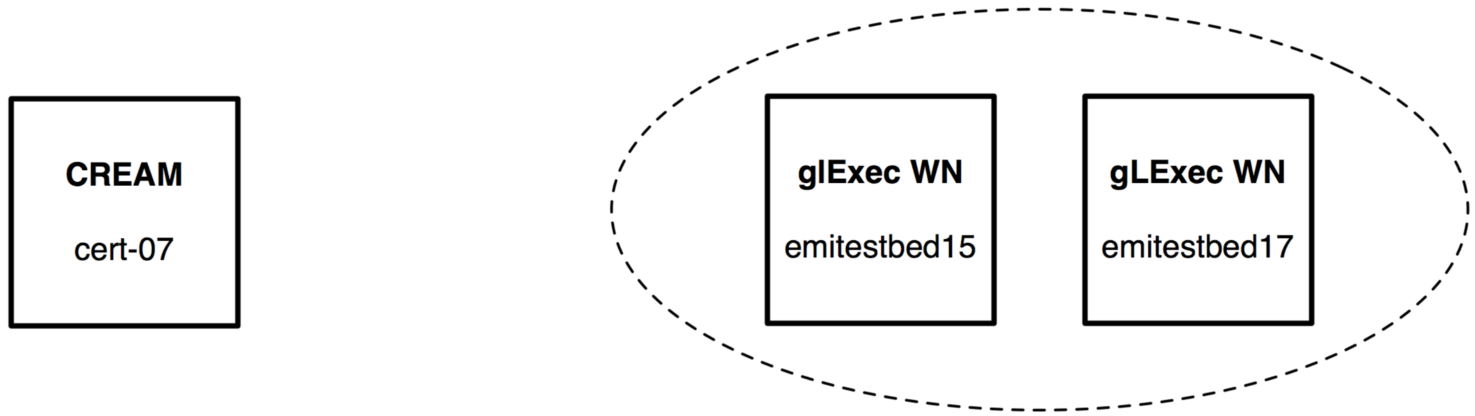
Reloading policies

- When policies are changed you need to
  - Tell the PDP to fetch the new policies from the PAP
    - `/etc/init.d/argus-pdp reloadpolicy`
  - Tell the PEPd it should clear its cache of decision responses from the PDP
    - `/etc/init.d/argus-pepd clearcache`

Demo

http://bit.ly/argus-policies

Testbed topology



Resource ID:
http://emitestbed.cnaf.infn.it/cert-07

Resource ID:
http://emitestbed.cnaf.infn.it/wn

- 1 CREAM CE
- 2 gLexec Worker Nodes
- The resource IDs will be used in Argus policies

Enabling a VO for job submission

Enabling a VO so that its jobs are authorized on CREAM and on gLexec on the WN.

```
resource "http://emitestbed.cnaf.infn.it/cert-07" {
    obligation "http://glite.org/xacml/obligation/local-environment-map" {}

    action ".*" {
        rule permit { vo="testers.eu-emi.eu" }
    }
}

resource "http://emitestbed.cnaf.infn.it/wn" {
    obligation "http://glite.org/xacml/obligation/local-environment-map" {}

    action ".*" {
        rule permit { vo="testers.eu-emi.eu" }
    }
}
```

Testing policies with PEP cli

```
pepcli
    --pepd "https://emitestbed10.cnaf.infn.it:8154/authz"
    -c /tmp/x509up_u507
    -r http://emitestbed.cnaf.infn.it/cert-07
    -a submit-job
    --cert /tmp/x509up_u507 --key /tmp/x509up_u507
```

YAIM service configurations (Argus, CREAM, gLexec)

Argus node site-info.def

```
# The Argus hostname
ARGUS_HOST=emitestbed10.cnaf.infn.it

# The DN of a trusted PAP administrator
PAP_ADMIN_DN="/C=IT/O=INFN/OU=Personal Certificate/L=CNAF/CN=Danilo Nicola Dongiovanni"

# Local mapping configuration
USERS_CONF=/root/siteinfo/users.conf
GROUPS_CONF=/root/siteinfo/groups.conf

# Space separated list of VOs supported by your site
VOS="testers.eu-emi.eu"
```

CREAM Argus configuration

```
CEMON_HOST=cert-07.cnaf.infn.it
CREAM_DB_USER=tester
CREAM_DB_PASSWORD=****
BLPARSER_HOST=cert-07.cnaf.infn.it
...
USE_ARGUS=yes
ARGUS_PEPD_ENDPOINTS="https://emitestbed10.cnaf.infn.it:8154/authz"
CREAM_PEPC_RESOURCEID="http://emitestbed.cnaf.infn.it/cert-07"
```

gLexec on the WN site-info.def

```
GLEXEC_WN_OPMODE="setuid"

GLEXEC_WN_SCAS_ENABLED="no"

GLEXEC_WN_ARGUS_ENABLED="yes"

ARGUS_PEPD_ENDPOINTS=”https://emitestbed10.cnaf.infn.it:8154/authz”

GLEXEC_WN_PEPC_RESOURCEID=”http://emitestbed.cnaf.infn.it/wn”
```

Documentation

- General documentation
  https://twiki.cern.ch/twiki/bin/view/EGEE/AuthorizationFramework
- Service Reference Card
  https://twiki.cern.ch/twiki/bin/view/EMI/ArgusSRC
- PAP admin CLI
- https://twiki.cern.ch/twiki/bin/view/EGEE/AuthZPAPCLI
- Simplified Policy Language
  https://twiki.cern.ch/twiki/bin/view/EGEE/SimplifiedPolicyLanguage

EUROPEAN MIDDLEWARE INITIATIVE

Thanks!

EMI is partially funded by the European Commission under Grant Agreement INFSO-RI-261611