

Introduction to Argus

*Andrea Ceccanti, Vincenzo Ciaschini
(Francesco Giacomini)*

*CCR & INFNGrid Workshop
Santa Tecla, 19th May 2010*

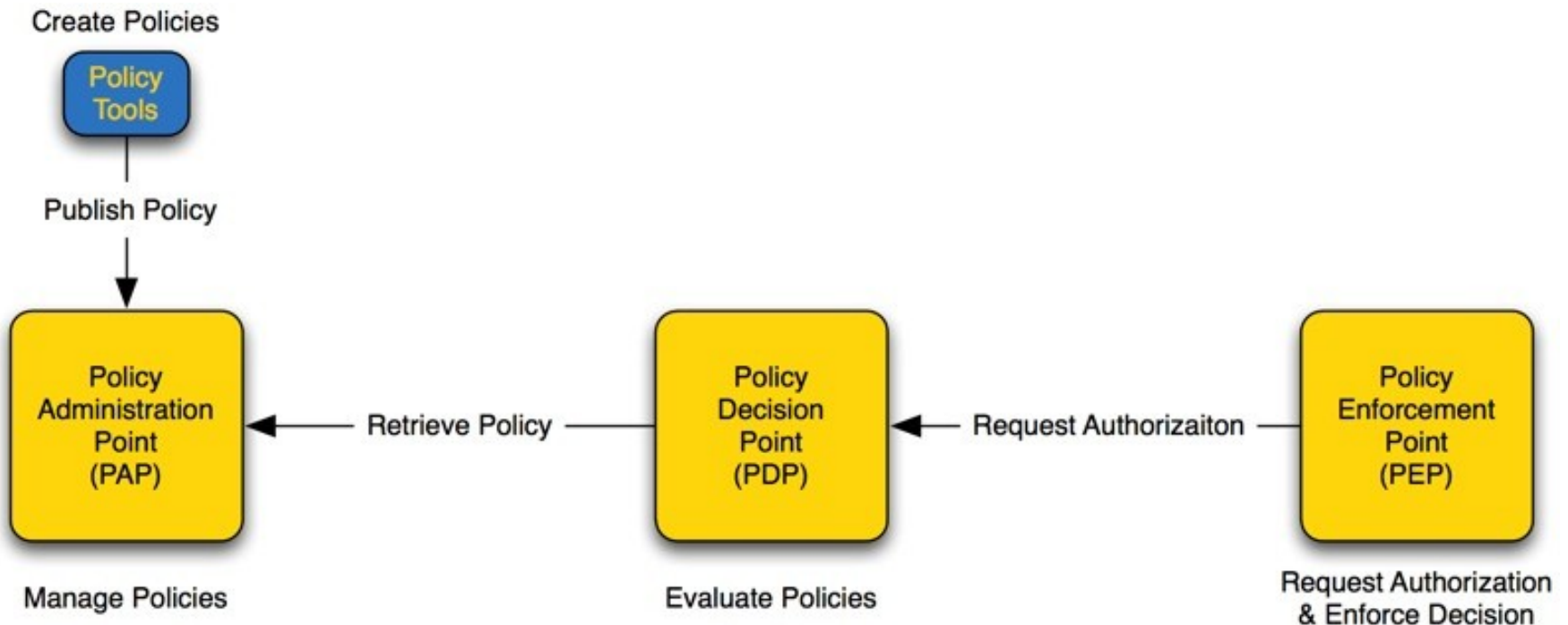
Can user **X**
perform action **Y**
on resource **Z**
?

- **Render consistent authorization decisions for different services**
- **Enable composition of policies from distributed sources**
 - local policy + INFN policy + OCST policy + VO policy = effective policy
 - Example: distributed banning/unbanning users becomes straightforward
- **Enable dynamic management of AuthZ policies**
 - without having to restart services
- **Flexible deployment model**
 - designed with HA in mind
- **Monitoring and auditing**

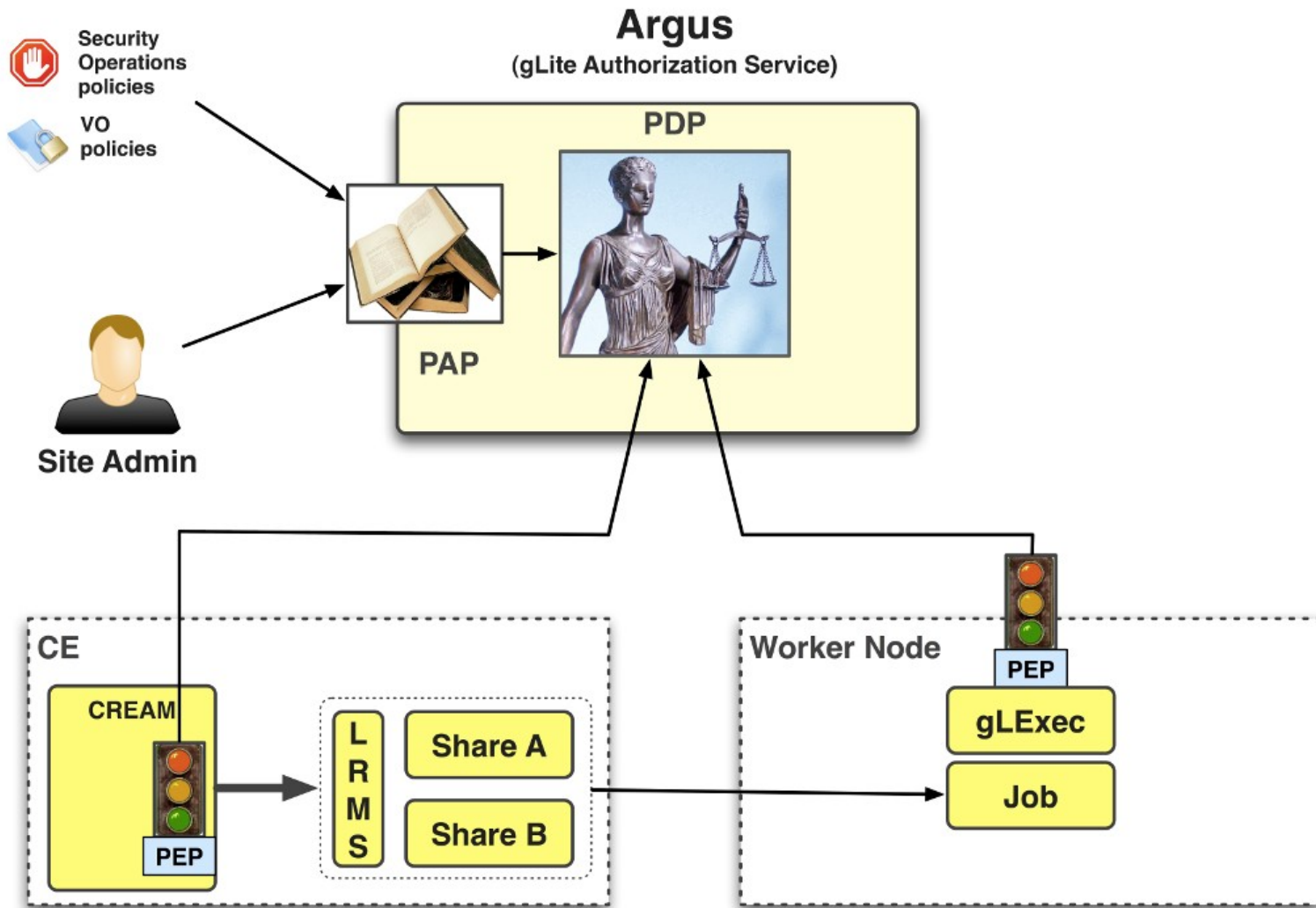
- **Argus policies contain rules that state which actions can be performed on which resources by which users**
 - Expressed in XACML v. 2.0
 - Difficult to read and write
- **A Simplified Policy Language (SPL) is available**

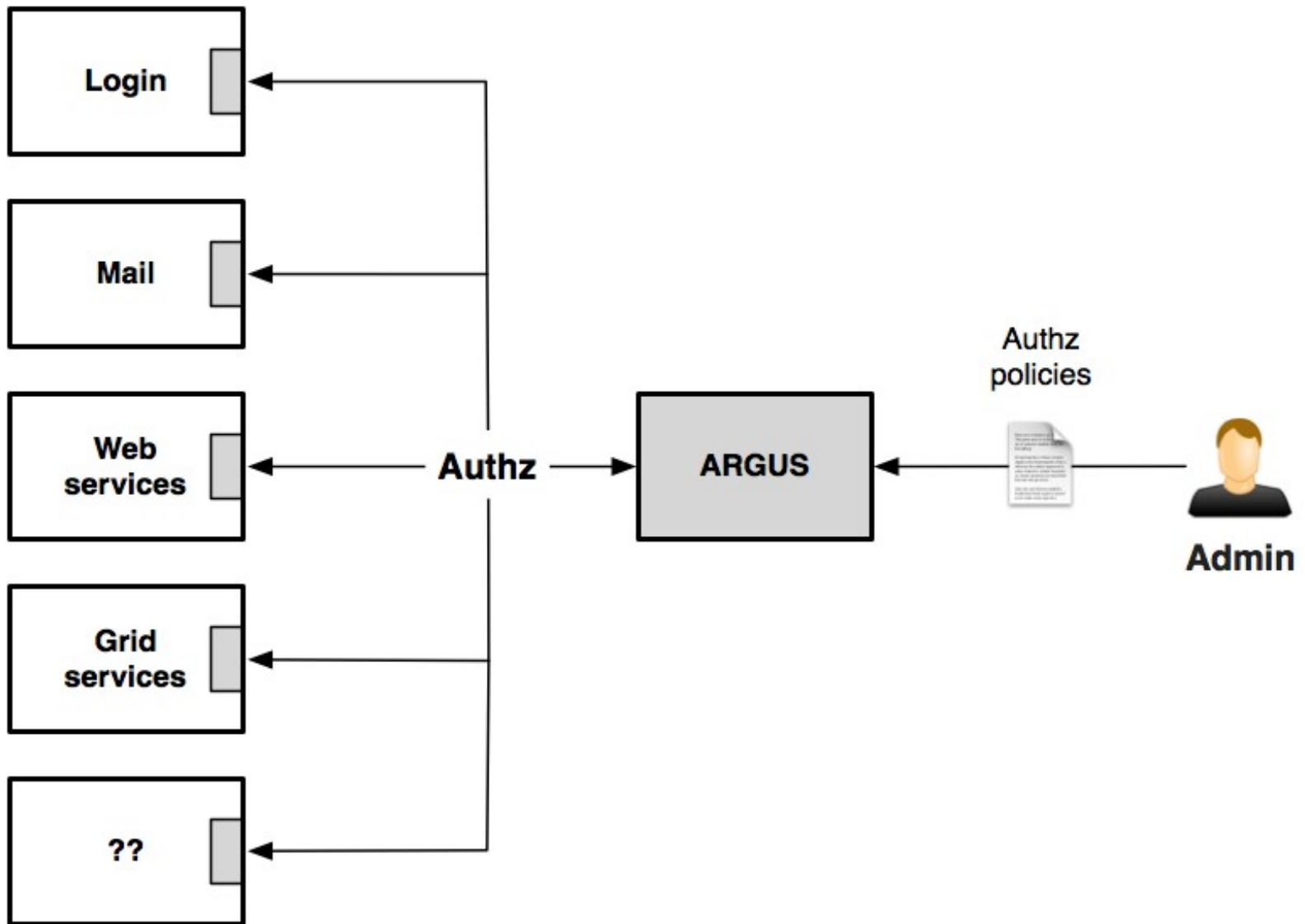
```
resource "devce.cnaf.infn.it:8443/cream-pbs-cert" {
  action "*" {
    rule permit {
      subject = "CN=Andrea Ceccanti,L=CNAF,OU=Personal Certificate, ..."
    }
  }
}
```

```
resource "*" {
  action "*" {
    rule deny {
      subject = "CN=Andrea Ceccanti,L=CNAF,OU=Personal Certificate, ..."
    }
  }
}
```



- **PAP:** author, store, manage and distribute policies
- **PDP:** evaluate requests against policies
- **PEP:** create request and enforce PDP decisions





```
resource "devce.cnaf.infn.it:8443/cream-pbs-cert" {  
  action ".*" {  
    rule permit {  
      subject = "CN=Andrea Ceccanti,L=CNAF,OU=Personal Certificate, ..."  
    }  
  }  
}
```



```
resource "bastion.cnaf.infn.it" {  
  action "login" {  
    rule permit {  
      username = "aceccanti"  
    }  
  }  
}
```