Argus and SAML

Christoph Witzig, Switch

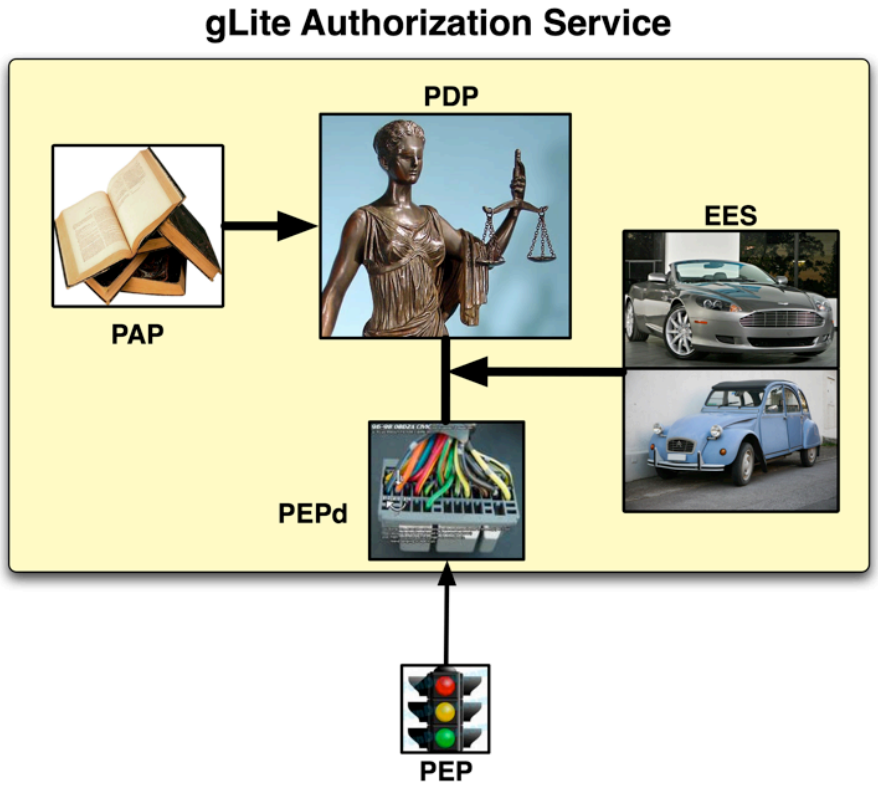
Andrea Ceccanti, INFN (Speaker)

EMI Security Workshop

May 2010, CERN

Argus Architecture

- **Clients can submit requests in two ways**
  - PEP-client (C or Java) sends data to the PEP daemon which creates XACML request based on the received information
    - Motivation : thin client, very few dependencies on the client library
  - Sending XACML requests directly to the PDP



- **The PDP and PEP Daemon use Policy Information Points (PIPs) to extract attributes used in the authorization decision**

Argus SAML support

- **Goal**
  - Allow Argus to render an authorization decision based on information from a SAML assertion

- **What needs to be done?**
  - Create a Policy Information Point for the PEP and PDP that can “decompose” a SAML assertion into XACML request context attributes

Open Questions

- **Who is responsible for validating the authenticity and integrity of the SAML assertion? Argus or the software invoking Argus?**
  - If Argus, what trust model is used?
- **Would a system that used SAML assertions still use X.509 client certificates to authenticate to the PEP and PDP?**
- **Which SAML assertions are we talking about?**
  - From an Identity Provider?
  - From VOMS-SAML (with attributes only)?
  - Embedded in a proxy?

Timeline

- **When should this functionality be available?**
  - Level of Effort:
    - ~ 2 person weeks for development and testing

- **Given this estimate, functionality can be added to pretty any release but open questions must be answered all before work starts**