MyProxy and VOMS

Daniel Kouril, CESNET

EGEE'06, Geneva

27th September 2006

Information Society and Media

MyProxy

- **Credential repository**
  - maintains long-term proxy certificates or even full credentials
  - issues short-time proxies
- **A few basic operations**
  - retrieval, renewal
- **Support of long-running jobs/operations**
  - The WMS periodically renews a proxy certificates and pushes it to the running job

MyProxy

- **Authentication based on SSL/TLS**
  - either using client‘s PKI credentials or password
  - other authN method supported via SASL
- **Authorization based on static lists of subject names**
  - stored in config file
  - independent lists for each operation
  - regular expressions allowed
- **Simple text based protocol**
  - sent over SSL/TLS secured channel

MyProxy and Trust

- **Relationship between MyProxy and its client is crucial**
  - clients must be authorized to access the repository
- **So far trust based on static configuration**
  - regular expressions aren‘t sufficient
  - a subject name of a service must be added on each change or addition
  - not flexible, could‘t profit from standard VO setup
- **WMS deployment**
  - WMS service must be allowed for `renewal` operations
  - installation of a ne WMS node requires changes to MyProxy

MyProxy and VOMS

- **VOMS support introduced recently**
  - the motivation was to ease the WMS deployment
  - MyProxy server analysis the client‘s VOMS attributes
  - allows to specify VOMS attributes instead of specifying subject names:
    - authorized_retrievers "FQAN:/voce/Role=Admin/Capability=NULL"
  - requires adding service certificates to VOMS machinery
- **Simplifies configuration**
- **Allows to use the standard VO mechanism for trust establishment**

MyProxy and VOMS

- **Verification of server‘s attributes**
  - not implemented
  - clients could verify the server
    - eg. when storing credentials
  - Mutual authorization again
- **Possible extensions to the myproxy protocol**
  - simple, backwards compatible
  - no proxies sent by the server

Services in VOMS

- **Maintaing service certificates in VOMS**
- **No technical issue**
- **Service should use two credentials**
  - VOMS-enabled when acting as a client for other services
  - Plain credentials for server authentication