Architecture Glite
Sécurité sur la Grille

Marseille

22 Octobre 2010

Sophie Nicoud (CNRS/CPPM)

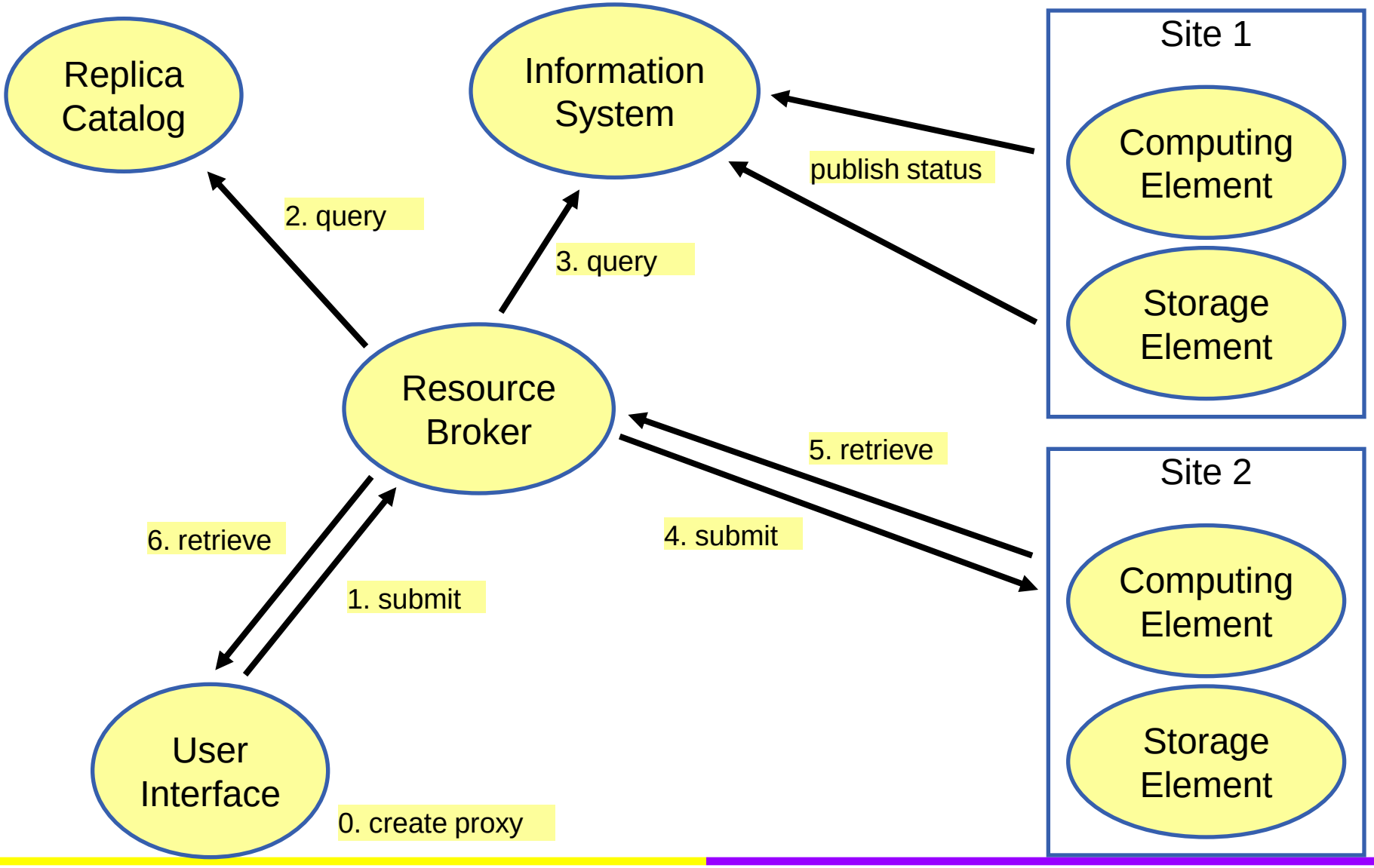
Architecture de GLite

- L'inter-logiciel est constitué d'une quinzaine de services différents
  - *L'interface utilisateur qui peut être une ligne de commande Linux ou un portail Web (UI : User Interface)*
  - *L'authentification et les autorisations sont gérées par l'Infrastructure de Sécurité de Grille, basée sur les certificats électronique X509v3 et les communautés d'utilisateurs. (CA : Certification Authority, VOMS : Virtual Organisation Management Service, VO : Virtual Organisation, GSI : Grid Security Infrastructure)*
  - *La gestion des ressources (RB : Resource Broker, WMS : Worload Management Service)*
  - *Le service d'information (BDII : Berkeley Database Information Index, IS : Information Service)*
  - *Les ressources de calcul (CE : Computing Element, WN : Worker Node)*
  - *Le stockage, les catalogues de données et protocoles de transfert (SE : Storage element, FTS : File Transfert Service, RC : Replica Catalog, LFC : Logical File Catalog)*
  - *Le service de comptabilité informatique (LB : Logging & Bookeeping)*
  - *…*

Soumission de job (1)

- L'utilisateur soumet son travail en utilisant une interface utilisateur (UI); ce service peut être un portail web (DIRAC, GILDA, ALien, Panda, ...) ou une ligne de commande Linux.
- Par cette interface l'utilisateur s'authentifie et présente ses autorisations.
- L'authentification est faite par certificat électronique X509v3.
- Puis, les autorisations sont vérifiées auprès du serveur VOMS de l'organisation virtuelle (VO) de l'utilisateur
- L'identité et les autorisations étant correctes, le job est présenté au gestionnaire des ressources (RB/WMS), qui en fonction de paramètres tels que par exemple : les ressources de calcul disponibles, l'emplacement des données, les programmes et librairies demandées et les autorisations, choisit le meilleur nœud de grille pour soumettre en queue le job.
- Le gestionnaire des ressources(RB/WMS) obtient ces informations par le service d'information (BDII).
- Je job est donc soumis à une ressource de calcul (CE) qui est en fait une ferme de calcul dans un des sites de la grille.
- Les données sont transférées par les protocoles de transfert de données (FTS), généralement GridFTP , des unités de stockage (SE) des VO vers ce site, grâce aux informations et aux fonctions de réplication des catalogues de données (LFC).
- Le déroulement du job est suivi grâce au service de comptabilité (LB), ce service peut être également utilisé au calcul des coûts de fonctionnement de la grille.
- Une fois le job terminé, l'utilisateur est informé de sa résolution et de la localisation des données résultantes via votre interface utilisateur.

Soumission de job (2)



Sécurité sur la Grille

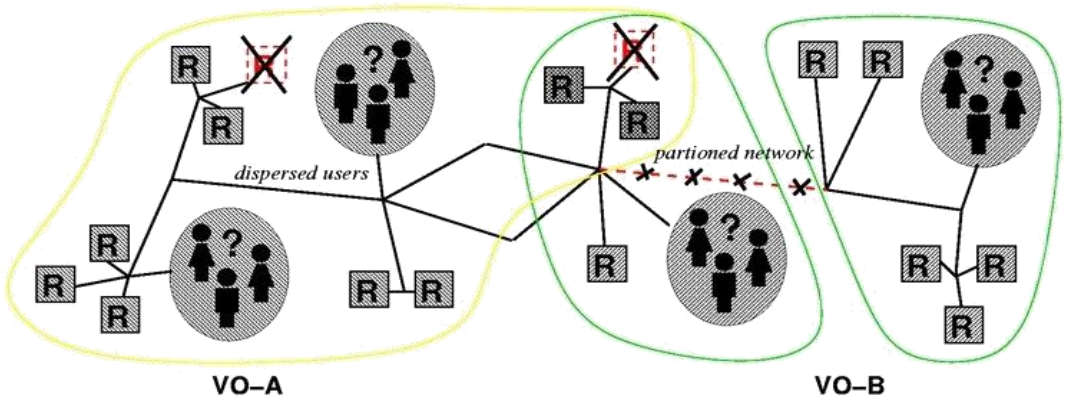
- **Un utilisateur pour utiliser la Grille doit posséder :**
  - ***Un certificat électronique personnel émis par son autorité de certification nationale (CA)***
  - ***Une entrée dans une Organisation Virtuelle (VO ou VOMS)***
  - ***Un compte sur une Interface Utilisateur ou sur un Service Web (UI)***
- **Authentification :**
  - ***GSI (Grid Security Infrastructure) basé sur les certificats X509v3 et les PKI***
  - ***Single-Sign-On***
  - ***L'utilisateur lors de l'authentification crée un proxy***
- **Autorisations :**
  - ***VO : Communauté d'utilisateurs ayant des buts communs utilisant et mettant à disposition des ressources communes***
  - ***Les utilisateurs ont des droits différents au sein de leur communauté (VO) grâce au service VOMS***

Les Autorités de Certification

- Problématique :
  - *Une seule CA par projet ou par partenaire => Pas gérable, peu sûr, problème de mise à l'échelle*
- Solution :
  - *Une CA par pays ou groupe de pays*
    => Établir des relations de confiance entre chaque CA
    => Coordination au niveau de chaque pays
  - *Catch-All CAs pour les pays sans CA nationales*
- En France :
  - *GRID2-FR géré par le CNRS*
- Politique de gestion des autorités : GRID PMA (Policy Management Authority)
  - *Etablir des obligations minimales pour les CA*
  - *Accréditer et auditionner les CA*
- IGTF, International Grid Trust Federation http://www.gridpma.org/
  - *Coordonne les PMA*
  - *Création de règles et chartes inter-PMA*
- EUGridPMA http://www.eugridpma.org
  - *Le pionnier, fondateur de l'IGTF et de ses règles et chartes*
  - *Couvre le continent Européen mais élargi à certaines CA dont le PMA n'est pas pleinement opérationnel*
- TAGPMA
  - *Amériques Sud et Nord*
- APGridPMA
  - *Asie et Pacifique*

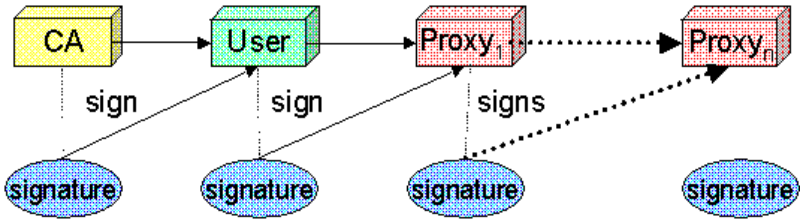
Les Autorisations

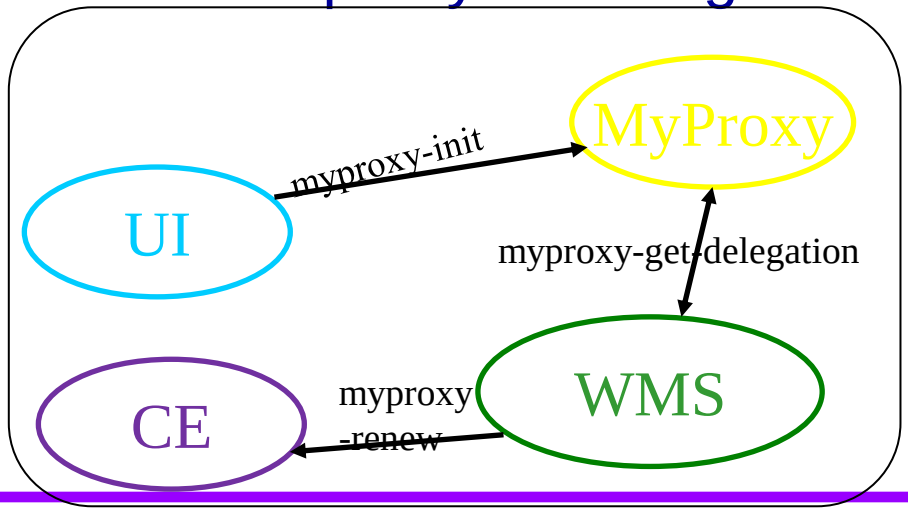
- Les VO : Communauté d'utilisateurs ayant des buts et des ressources en commun
- Chaque VO à ses règles d'utilisation et sa politique de sécurité
- Les VOMS
  - La base de données de la VOMS contient l'ensemble des membres avec leur niveau d'autorisation
  - Un utilisateur peut avoir plusieurs niveaux d'autorisation dans chaque VOMS et faire partir de plusieurs VOMS
  - Les droits des membres d'une VOMS sont en fonction de leur groupe ou rôle
  - Les groupes, rôles et droits sont inclus dans le proxy de l'utilisateur lorsque celui s'authentifie



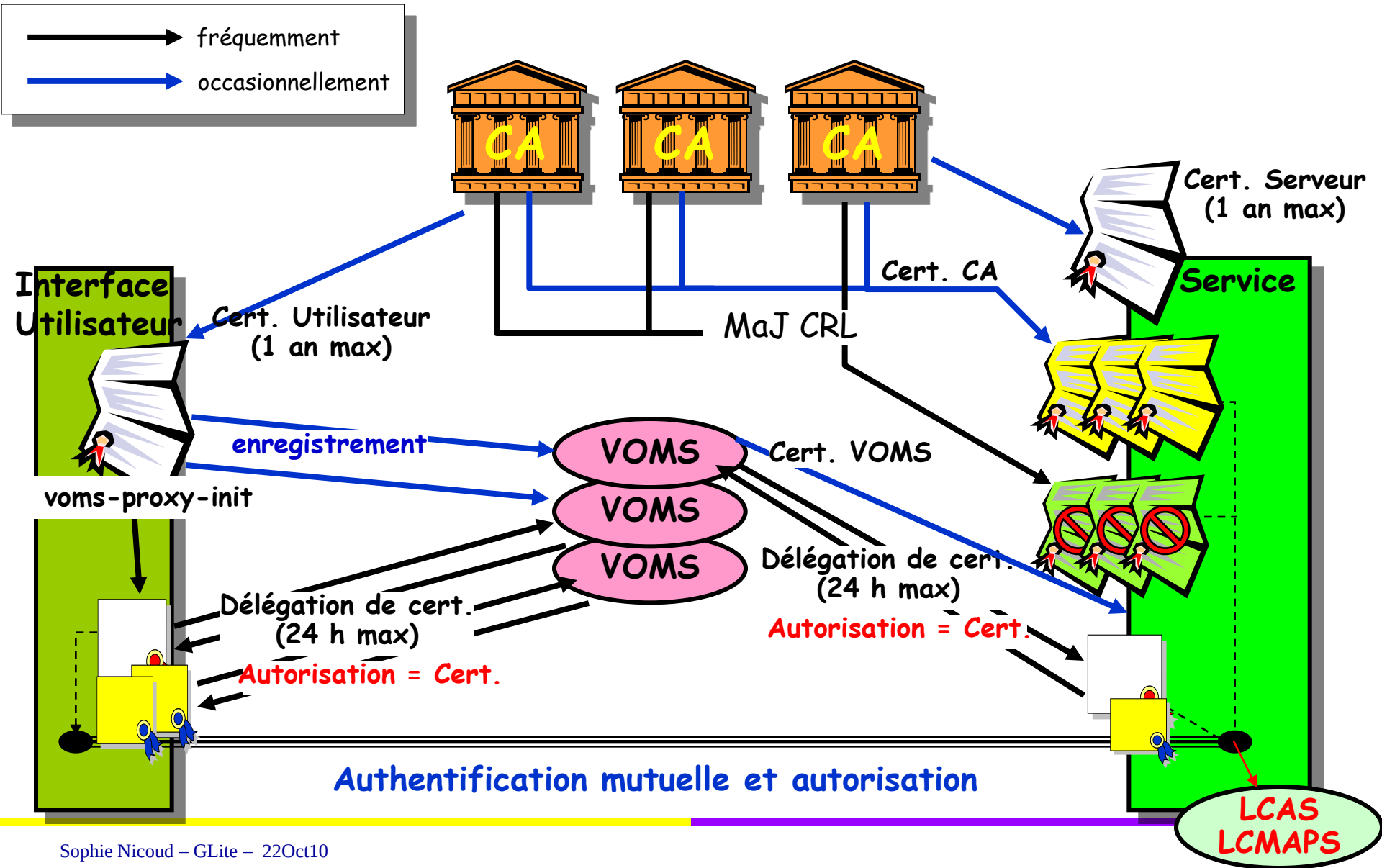
Proxy

- Certificat proxy
  - *Certificat à durée de vie courte, contenant sa clé privée, signé avec le certificat de l'utilisateur*
  - *Un Proxy peut se déplacer sur le réseau*
- Un proxy a une vie limitée (défaut à 12 h)
- Le service MyProxy permet de créer des proxys de longue durée (défaut à 7 jours)





Mécanisme d'authentification et d'identification



Liens

- **Autorités de Certification**
  - ***http://www.igtf.net***
  - ***http://eugridpma.org***
  - ***http://igc.services.cnrs.fr/GRID2-FR/***
- **VOMS**
  - ***https://edms.cern.ch/file/572406/1/user-guide.pdf***
  - ***https://cclcgvomsli01.in2p3.fr:8443/voms/vo.formation.idgrilles.fr***
- **MyProxy**
  - ***http://grid.ncsa.uiuc.edu/myproxy/doc.html***
- **gLite security infrastructure**
  - ***https://edms.cern.ch/document/935451/2***
- **Grid Security Infrastructure**
  - ***http://www.globus.org/grid_software/security/***