Sécurité sur le GRID

Edith Knoops
(CNRS/CPPM)

Tutorial EGEE
LAPP Annecy
26 septembre 2007

Plan

- Que faut-il pour travailler sur la Grille de Calcul ?
- La sécurité sur la Grille de Calcul
  - Grid Security Infrastructure (GSI)
- Authentification
  - Les certificats électroniques
  - Les fédérations d'Autorités de Certification
  - GRID-FR
- Autorisation
  - Les Organisations Virtuelles
  - Mécanismes et architectures
- Les proxys
  - Les proxys de courte durée
  - Les proxys de longue durée

Que faut-il pour travailler sur la Grille de Calcul ?

Enabling Grids for E-science in Europe

- Un utilisateur pour utiliser le GRID doit posséder :

- Un certificat électronique personnel

- Une entrée dans une Organisation Virtuelle (VO ou VOMS)

- Un compte sur une Interface Utilisateur ou sur un Service Web (UI)

Authentification/Autorisation

- Authentification => Certificat électronique X509 (CA)
  - Qui est qui ?
- Autorisation => Organisation Virtuelle (VO ou VOMS)
  - Qui a le droit ?
- Accès au GRID => Interface Utilisateur ou Service Web (UI)
- Audit sécurité
  - QUI fait QUOI et QUAND ?
- Comptabilité
  - COMBIEN de ressources consomme Mr ou Mme X ou la VO Y ?
- Facturation possible

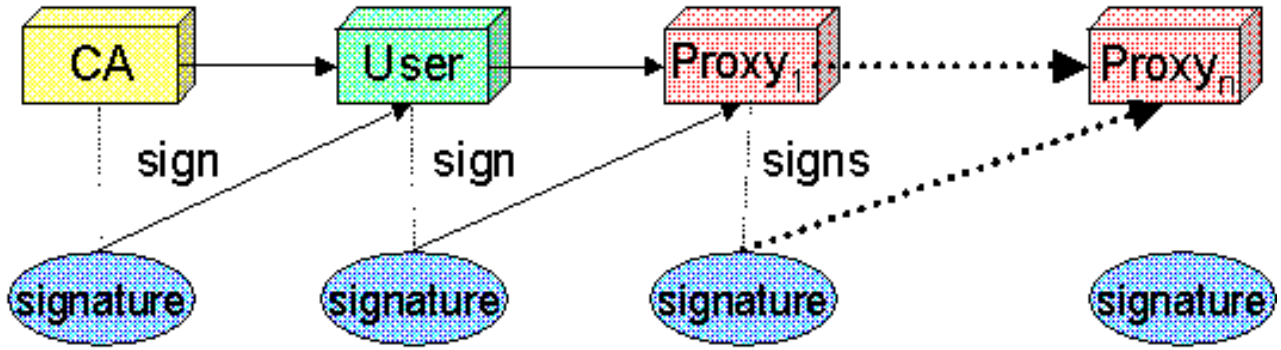
Plan

Enabling Grids for E-science in Europe

- La sécurité sur la Grille de Calcul
  - Grid Security Infrastructure (GSI)

Grid Security Infrastructure (GSI)

- Un standard pour les logiciels de Grille de Calcul
- Basé sur les certificats X509v3 et les PKI
- Implémente :
  - Single sign-on: le mot de passe n'est donné qu'une seule fois
  - Délégation: un service peut-être utilisé au nom d'une autre personne c-a-d autoriser une autre entité à utiliser son authentification et ses autorisations
  - Authentification mutuelle: le destinataire et l'émetteur s'authentifient
- Introduction des certificats proxy
  - Certificat à durée de vie courte, contenant la clé privée, signé avec le certificat de l'utilisateur
  - Un Proxy peut se déplacer sur le réseau



Plan

Enabling Grids for E-science in Europe

- Authentification
  - Les certificats électroniques
  - Les fédérations d'Autorités de Certification
  - GRID-FR

Qu'est qu'un certificat électronique X509v3 ?

- Repose sur l'utilisation des algorithmes asymétriques
- et l'accréditation par un tiers de confiance, l'Autorité de Certification (CA)
- C'est un couple de clés indissociables
  - Les clés sont générées ensembles
  - Impossibilité de retrouver une clé par rapport à l'autre
- Un certificat X509v3 peut être issu pour
  - Une personne physique (certificat personnel)
  - Une machine (certificat de hôte)
  - Un programme (certificat de service)
- Le certificat a une période de validité
- Il est composé d'une clé publique et d'une clé privée
- La clé publique
  - Signée par l'Autorité de Certification après vérification de l'identité du destinataire
  - Publiée sur le réseau via le service de publication de la CA
  - Dans le langage courant, elle est appelée *certificat*

- La clé privée
  - Conservée sur le poste de l'utilisateur ou sur la machine
  - Chiffrée et protégée par un mot de passe

Certificat X509v3 (1)

- Informations importantes contenues dans un certificat (clé publique):
  - Le sujet ou DN du certificat
  - Le numéro de série du certificat
  - La période de validité du certificat
  - L'Autorité de Certification émettrice
  - La clé publique
  - Des extensions X509v3
    - Les utilisations autorisées du certificat
    - L'email
    - ...
  - La signature de la CA émettrice
- Il faut toujours avoir :
  - La Liste des Certificats Révoqués (CRL) émise par la CA
  - Le certificat de la CA émettrice

Certificat X509v3 (2)

- Il existe plusieurs formats de représentation des certificats
  - PKCS12
    - Extensions .p12 ou .pfx
    - La clé privée et la clé publique sont dans un même fichier
    - Le fichier est chiffré et protégé par un mot de passe
    - La plupart des CA délivrent les certificats personnels dans ce format
  - PEM
    - Extensions .pem ou .crt et .key
    - La clé privée et la clé publique sont dans 2 fichiers distincts
    - Le fichier contenant la clé privée est chiffré et protégé par un mot de passe
    - C'est ce format que nous utilisons sur la Grille de Calcul

Un certificat X509v3 (1)

Enabling Grids for E-science in Europe

```
# openssl x509 -text -noout -in usercert.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 656 (0x290)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=FR, O=CNRS, CN=GRID-FR
        Validity
            Not Before: Feb  8 10:04:45 2007 GMT
            Not After : Feb  8 10:04:45 2008 GMT
        Subject: O=GRID-FR, C=FR, O=CNRS, OU=CPPM, CN=Edith Knoops
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:b9:8d:52:15:ee:80:d8:8f:3c:a7:1f:fb:59:6d:
```

- Numéro de série
- CA émettrice
- Période de validité

- Sujet
- Clé publique

Un certificat X509v3 (2)

Enabling Grids for E-science in Europe

X509v3 extensions:

X509v3 Basic Constraints: critical

CA:FALSE

Netscape Cert Type:

SSL Client, S/MIME, Object Signing

X509v3 Key Usage: critical

Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment, Key Agreement

- Extensions X509v3
  - Autorisations d'utilisation

X509v3 Certificate Policies:

Policy: 1.3.6.1.4.1.10813.1.1.8.1.0

X509v3 Subject Alternative Name:

email:knoops@cppm.in2p3.fr

X509v3 CRL Distribution Points:

URI:http://crls.services.cnrs.fr/GRID-FR/getder.crl

1.3.6.1.4.1.7650.1:

unicoreClient

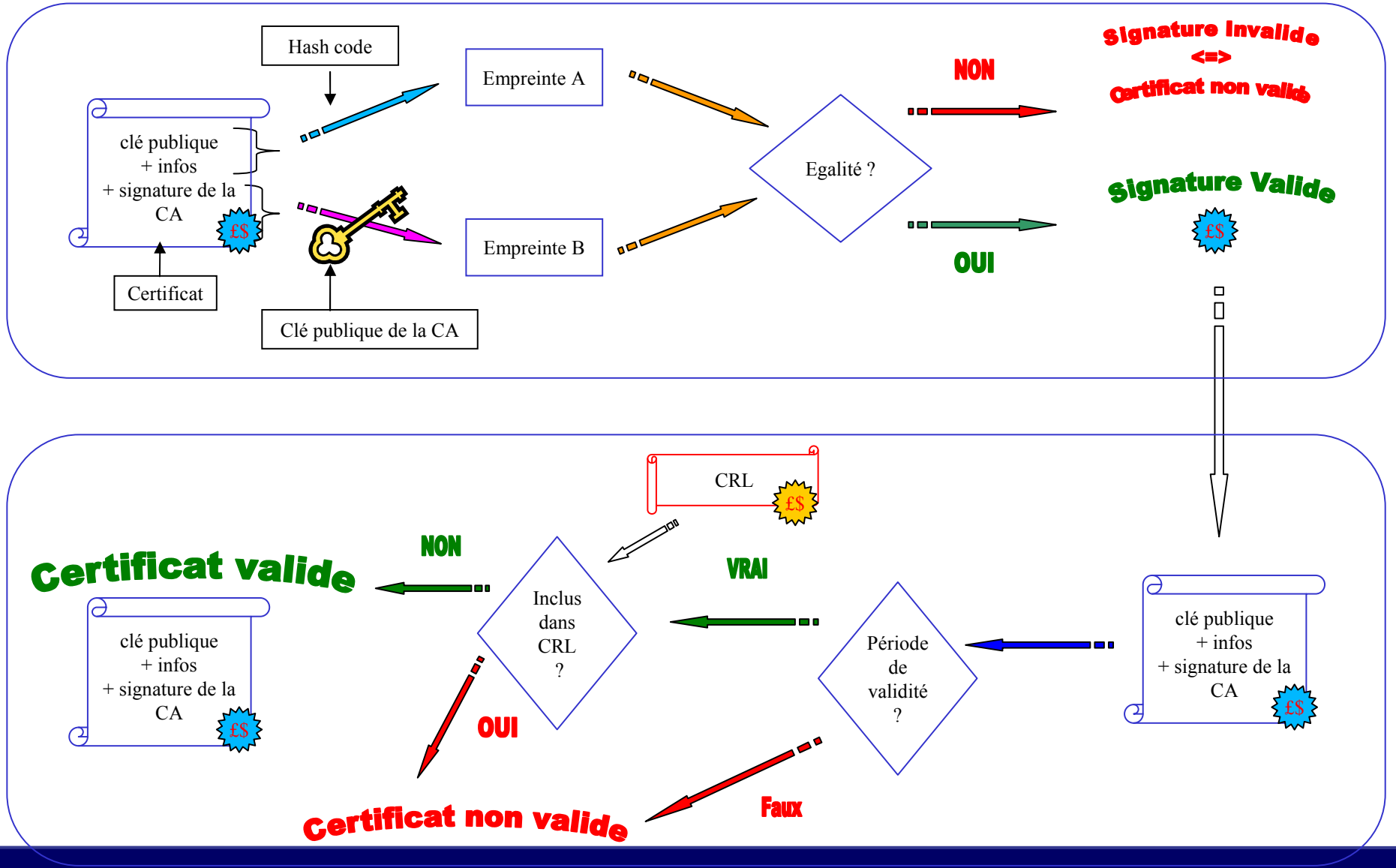
- Extensions X509v3
  - Version CP/CPS de la CA
  - Email
  - CRL

Signature Algorithm: sha1WithRSAEncryption

7a:ea:e5:96:d6:cb:2f:2e:a6:9c:1d:06:55:8a:af:2a:7a:1c:

- Signature de la CA

Vérification d'un certificat



openssl

- Convertir un certificat du format PKCS12 au format PEM
  - Obtenir la clé privée

openssl pkcs12 -nocerts -in cert.p12 -out userkey.pem

  - Obtenir la clé publique

openssl pkcs12 -clcerts -nokeys -in cert.p12 -out usercert.pem

- Visualiser une clé publique
  - Format PEM

openssl x509 -text -noout -in usercert.pem

  - Format PKCS12

openssl pkcs12 -info -in cert.p12

- Changer le mot passe de la clé privée

openssl rsa -in userkey.pem

Les Autorités de Certification

- Problématique :
  - Une seule CA par projet => Pas gérable, peu sûr
  - Une CA par partenaire => 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
    - Pays sans CA nationales
- Politique de gestion des autorités : GRID PMA
  - PMA, Policy Management Authority
  - Etablir des obligations minimales pour les CA
  - Accréditer les CA
  - Auditionner les CA

Organisation des PMA

- IGTF, International Grid Trust Federation
  - Coordonne les PMA
  - Création de règles et chartes inter-PMA
  - http://www.gridpma.org/
- EUGridPMA
  - 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 (US, Canada, Chine, Taiwan, ...)
  - http://www.eugridpma.org
- TAGPMA
  - Amériques Sud et Nord
  - 3 CA en Amérique du nord, Plusieurs en cours d'accréditation sur l'Amérique du Sud
- APGridPMA
  - Asie et Pacifique
  - 10 CA, Autralie, Japon, Chine, Taiwan, Corée

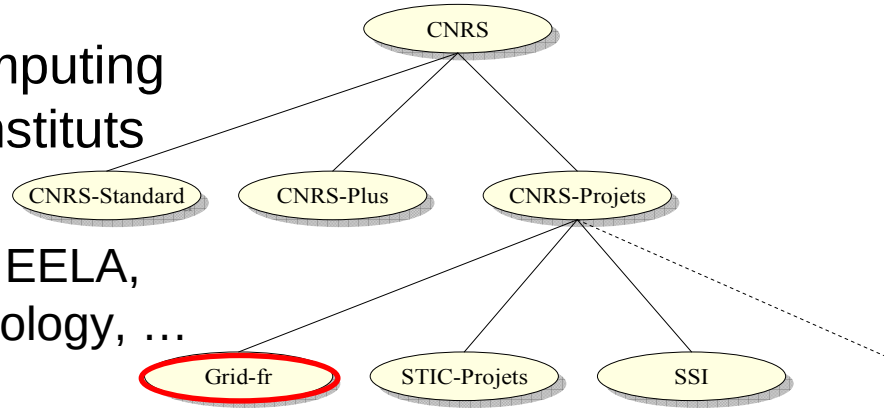
Obligations minimales

- CRL
  - Emettre une CRL dès qu'un certificat est révoqué
  - Validité maximum d'un mois
  - Ré-émission de la CRL 7 jours avant son expiration
- Machine CA
  - Dédiée, off-line
  - Protection des clés
- Espace de nommage des sujets de certificats UNIQUE
- Architecture de la PKI
  - Une CA par pays ou groupe de pays
  - Une CA dédiée aux projets de Grille de Calcul
- …

http://eugridpma.org/guidelines/ : Obligations minimales
http://eugridpma.org/charter/ : Définition du groupe

GRID-FR. Pourquoi ?

- Répondre aux obligations de EUGridPMA
- Sous-CA du CNRS :
  - Dédiée aux projets de GRID Computing dans lesquels le CNRS ou des instituts Français sont impliqués
    - EGEE, LCG, DEISA, Grid 5000, EELA, ILDG, E-Sciences, Integrative Biology, …



  - Délivre des certificats personnels, de services et serveurs aux :
    - Instituts publics et organismes privés Français
    - Instituts publics et organismes privés étrangers, non HEP, ne disposant pas d'une CA accréditée GRID.

GRID-FR. Spécificités

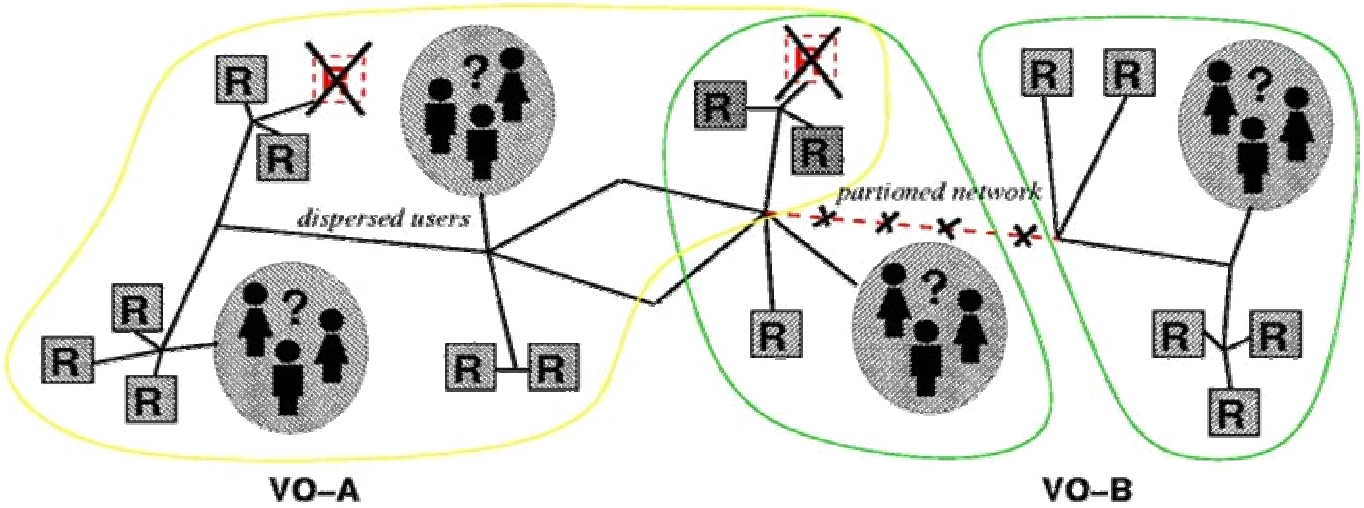
- Spécificités par rapport aux autres sous-CA du CNRS :
  - Sujet des certificats distinctif et unique
  - Possibilité d'avoir des sujets de certificat :
    - /O=GRID-FR/C=FR/O=CNRS/OU=UREC/CN=ldap/monserveur
  - Certificats émis à d'autres instituts que le CNRS, d'autres pays, ...
  - Extensions X509v3 spécifiques aux GRIDs
  - Algorithme de signature de la CA GRID-FR
    - SHA1
  - CRL
    - Générée chaque nuit
    - Valide 1 mois
    - Serveur spécifique pour le téléchargement
      - **crls.services.cnrs.fr**
  - Traduction en Anglais des pages, des formulaires et des emails
- Bref, GRID-FR suit les obligations de EUGridPMA

Plan

- Autorisation
  - Les Organisations Virtuelles
  - Mécanismes

Autorisation

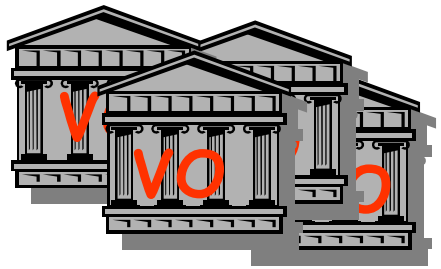
- Organisations Virtuelles (VO)
  - Ensemble d'individus ayant des buts communs
  - Utilisateurs
  - Ressources



A set of individuals or organisations, not under single hierarchical control, (temporarily) joining forces to solve a particular problem at hand, bringing to the collaboration a subset of their resources, sharing those at their discretion and each under their own conditions.

Organisations Virtuelles (1)

- Les utilisateurs sont regroupés par expérience scientifique, laboratoire, région ou projet
  - Expériences : Biomed, gene, Alice, Atlas, Babar, LHCb, ESR, EGEODE, ...
  - Laboratoires, régions : vo.dapnia.cea.fr, vo.lal.in2p3.fr, cppm, vo.grif.fr, ...
  - Projets : Ambrace, infngrid, GridPP, auvergrid, ...
  - Autre : dteam, ...
- https://cic.in2p3.fr/index.php?id=vo



- Un administrateur par Organisation Virtuelle
  - C'est le gestionnaire des utilisateurs de sa VO

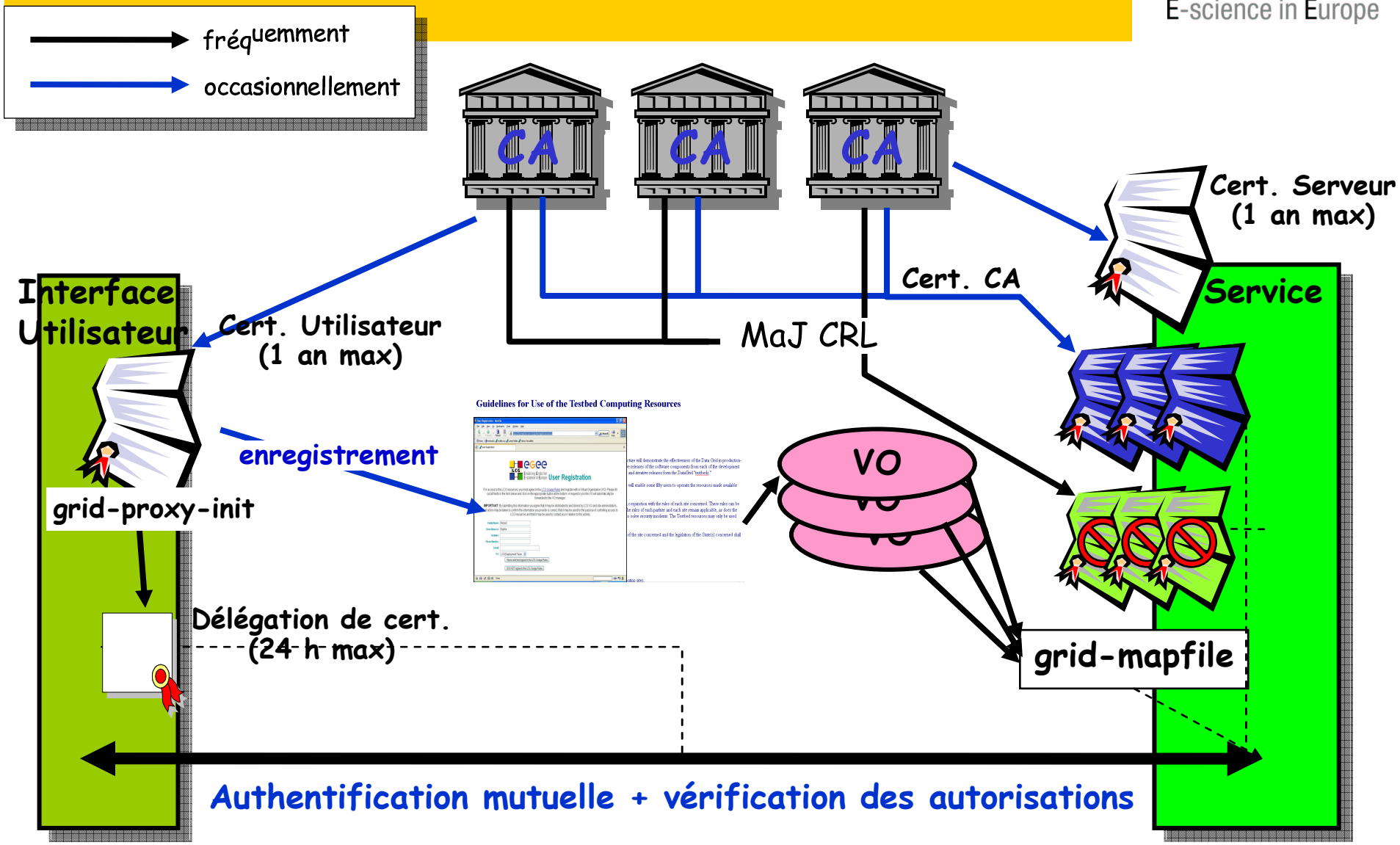
- Les sites se déclarent utilisables par X,Y ou Z VO
- Des droits spécifiques peuvent être données au niveau de chaque site par l'administrateur de celui-ci.
  - Interdire l'accès à un groupe d'utilisateur en fonction de leur sujet de certificat

Les VO LDAP

- Au niveau de chaque site, un compte ou UID/GID est affecté à chaque utilisateur en fonction de sa VO
- Cet UID/GID est pris dans un pool de compte mis à disposition pour chaque VO
- Actuellement, il existe 2 types de VO : Les VO LDAP et les VOMS
- **Les VO LDAP**
  - Les plus anciennes, le serveur LDAP de la VO contient l'ensemble des membres de celle-ci
  - Un utilisateur ne peut faire partir que d'une VO
  - Tous les membres d'une VO ont les mêmes droits
  - L'utilisateur s'authentifie avec : **grid-proxy-init**
  - Le fichier d'autorisation, grid-mapfile, généré périodiquement sur chaque site fait correspondre à chaque sujet de certificat un pool de compte

```
"/O=GRID-FR/C=FR/O=CNRS/OU=CC-LYON/CN=Sylvain Reynaud" .dte
"/O=GRID-FR/C=FR/O=CNRS/OU=CPPM/CN=Alexandre Rozanov" .atl
"/O=GRID-FR/C=FR/O=CNRS/OU=CPPM/CN=Andrei Tsaregorodtsev" lhcs
```

Architecture avec les VO LDAP



Les VOMS (1)

Enabling Grids for E-science in Europe

- **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, 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 avec :
    voms-proxy-init --voms <vo-name>
  - Les autorisations sont exprimées par **FQAN*** et placées dans les attributs du proxy généré
    <group>/Role=[<role>][/Capability=<capability>]

*FQAN : Fully Qualified Attributes Name

Les VOMS (2)

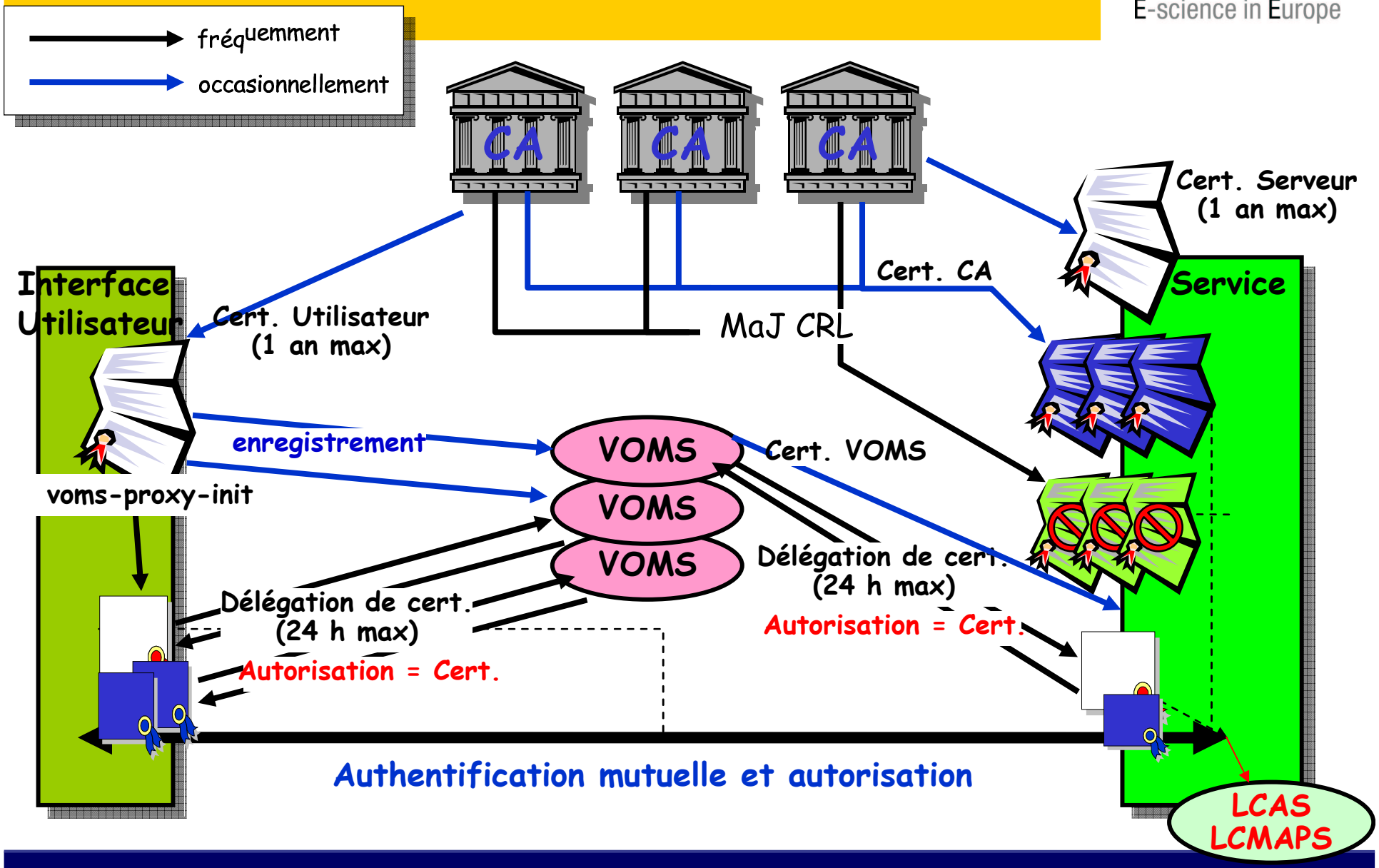
- Les groupes
  - Les groupes sont hiérarchiques, profondeur non limitée
  - Permet de moduler les droits des membres de la VOMS en fonction de leur groupe
  - Le groupe par défaut est /<vo-name>
- Les rôles
  - Software manager, VO-Administrator, Production, …
  - Les rôles ne sont pas hiérarchiques : il n'existe pas de sous-rôle
  - Les rôles doivent être explicitement spécifiés lors de la création du proxy
  - En déroulement normal les rôles ne sont pas pris en compte
- Les attributs du proxy sont analysés par chaque site accédés grâce à **LCAS** et **LCMAPS**

Les VOMS (3)

- LCMAPS
  - Fait correspondre le sujet de certificat en fonction des attributs du proxy à un compte utilisateur local au site (UID/GID)
- LCAS
  - Vérifie dans le grid-mapfile si l'utilisateur est autorisé ou interdit sur ce site
- Le fichier d'autorisation, grid-mapfile, généré périodiquement sur chaque site fait correspondre à chaque VOMS/group/rôle un pool de compte ou un compte

```
"/VO=dteam/GROUP=/dteam" .dte
"/VO=dteam/GROUP=/dteam/ROLE=NULL" .dte
"/VO=dteam/GROUP=/dteam/ROLE=NULL/CAPABILITY=NULL" .dte
"/VO=dteam/GROUP=/dteam/ROLE=lcgadmin" dtes
"/VO=dteam/GROUP=/dteam/ROLE=lcgadmin/CAPABILITY=NULL" dtes
"/VO=dteam/GROUP=/dteam/ROLE=production" dtep
"/VO=dteam/GROUP=/dteam/ROLE=production/CAPABILITY=NULL" dtep
```

Architecture avec les VOMS



Plan

- Les proxys
  - Les proxys de courte durée
  - Les proxys de longue durée

Proxy de courte durée - VO

- Obtenir des informations sur le certificat utilisateur
  - **`grid-cert-info[-help] [-file certfile] [OPTION]...`**

    `-all`tout le certificat

    `-subject | -s` sujet

    `-issuer | -I` émetteur

    `-startdate | -sd` début de validité

    `-enddate | -ed` fin de validité
- Créé un certificat proxy
  - **`grid-proxy-init`**
- Détruire un certificat proxy
  - **`grid-proxy-destroy`**
- Obtenir des informations sur un certificat proxy
  - **`grid-proxy-info`**

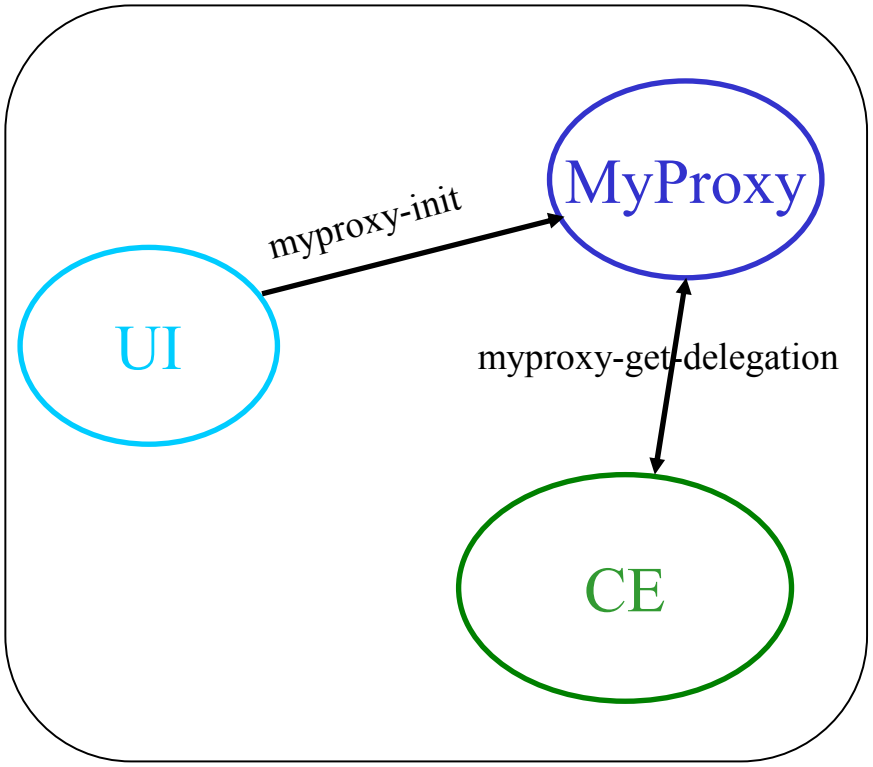
Proxy de courte durée - VOMS

- Créer un proxy
  - **voms-proxy-init - -voms <vo-name>**
- Créer un proxy en spécifiant un groupe
  - **voms-proxy-init –-voms <vo-name>:/group/**
- Créer un proxy en spécifiant un rôle
  - **voms-proxy-init –-voms <vo-name>:[/group]/role=production**
- Obtenir des informations sur un proxy
  - **voms-proxy-info**
- Détruire un proxy
  - **voms-proxy-destroy**

Proxy de longue durée (1)

- Un proxy a une vie limitée (défaut à 12 h)
  - C'est une mauvaise idée de prolonger la vie d'un proxy
- Cependant, un job peu avoir besoin d'un proxy avec une vie plus longue

- Le service myproxy permet de créer des proxys de longue durée (défaut 7 jours)
- Les proxys créés sont conservés par myproxy



Proxy de longue durée (2)

- Pour l'instant, MyProxy ne tient pas compte des extensions VOMS
- La prise en compte des rôles et groupes a été annoncée à EGEE'06
- Stocker un proxy dans la base du serveur MyProxy
  - **`myproxy-init –d -n`**
- Obtenir des informations sur un proxy stocké
  - **`myproxy-info -v`**
- Récupérer un proxy stocké
  - **`myproxy-get-delegation`**
- Détruire un proxy stocké
  - **`Myproxy-destroy`**

Liens

- Autorités de Certification
  - http://gridpma.org/
  - http://www.eugridpma.org/
  - http://marianne.in2p3.fr/ca/
- VOMS
  - https://edms.cern.ch/file/572406/1/user-guide.pdf
- MyProxy
  - http://grid.ncsa.uiuc.edu/myproxy/doc.html