Sécurité sur EGEE, indications utilisateurs

Sophie Nicoud **(CNRS/IGH**, anciennement **UREC)**
David Weissenbach **(CNRS/IPGP)**

Tutoriel EGEE utilisateur

Observatoire de Meudon
10 – 12 Déc 2008

Information Society and Media

Plan

Enabling Grids for E-science in Europe

- Que faut-il pour travailler sur la Grille de Calcul EGEE ?
- La sécurité sur la Grille de Calcul
  - Grid Security Infrastructure (GSI)
- Authentification
  - Les certificats électroniques
  - Les fédérations d'Autorités de Certification
- 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 accéder à EGEE doit posséder :

- Un certificat électronique personnel

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

- Un compte sur

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

Authentification/Autorisation

Enabling Grids for E-science in Europe

- 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)

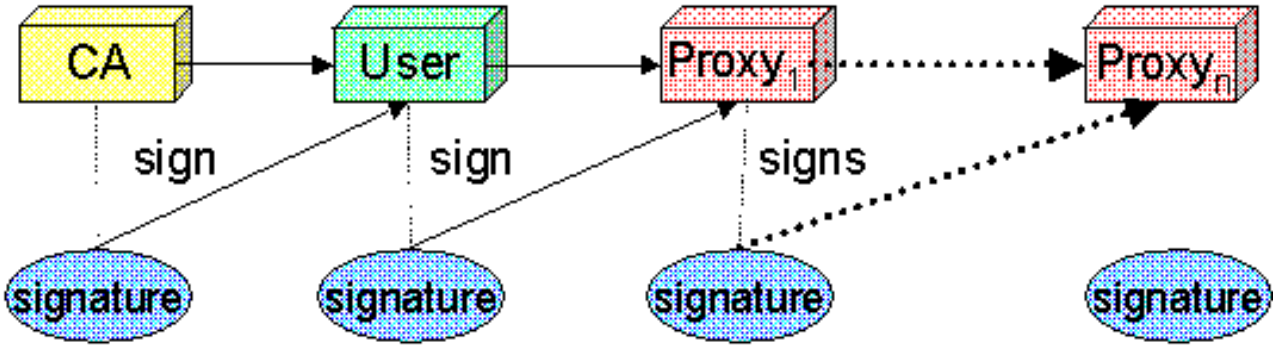
- Audit sécurité
  - QUI fait QUOI et QUAND ?
- Comptabilité (facturation?)
  - COMBIEN de ressources consomme Mr ou Mme X ou la VO Y ?

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

GSI ii

- Introduction des certificats 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



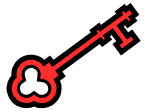
Qu'est qu'un certificat électronique X509v3 ?

Enabling Grids for E-science in Europe

Repose sur l'utilisation de la cryptographie asymétrique (RSA) et l'accréditation par un tiers de confiance, l'Autorité de Certification (CA)

- Un certificat X509v3 peut être issu pour
  - Une personne physique (certificat personnel)
  - Une machine (certificat hôte) / un programme (certificat de service)
- C'est un couple de clés indissociables
  - Les clés sont générées ensembles
  - Impossibilité de retrouver une clé à partir l'autre
- Le certificat a une période de validité
- 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 (<=> la prunelle de vos yeux)
  - Conservée par le navigateur de l'utilisateur et dans son *home* sur l'UI
  - 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
  - le DN de l'Autorité de Certification émettrice
  - La clé RSA publique
  - Des extensions X509v3
    - Les utilisations autorisées du certificat, adresse mail, ...
  - La signature de la CA émettrice
- Pour vérifier la validité d'un certificat, il faut toujours avoir :
  - La Liste des Certificats Révoqués (CRL) émise par la CA
  - Le certificat (auto-signé) de la CA émettrice

Certificat X509v3 (2)

Enabling Grids for E-science in Europe

- Les certificats sont conservés dans des **FICHIERS.**
- Il existe plusieurs formats de représentation des certificats
  - PKCS12 (format navigateur web)
    - 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 (format « grille »)
    - 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

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 2006 GMT
            Not After : Feb  8 10:04:45 2007 GMT
        Subject: O=GRID-FR, C=FR, O=CNRS, OU=UREC,
CN=Sophie Nicoud
        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 (DN)
- Clé publique

Un certificat X509v3 (2)

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

X509v3 Certificate Policies:
Policy: 1.3.6.1.4.1.10813.1.1.8.1.0
X509v3 Subject Alternative Name:
email:Sophie.Nicoud@urec.cnrs.fr
X509v3 CRL Distribution Points:
URI:http://crls.services.cnrs.fr/GRID-FR/getder.crl
1.3.6.1.4.1.7650.1:
unicoreClient
Signature Algorithm: sha1WithRSAEncryption
7a:ea:e5:96:d6:cb:2f:2e:a6:9c:1d:06:55:8a:af:2a:7a:1c:

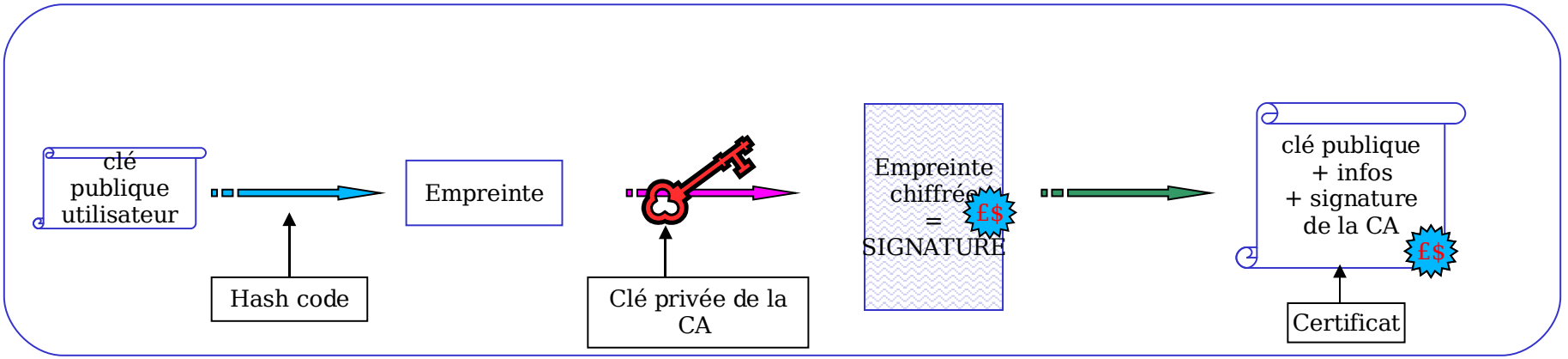
- Extensions X509v3
  - Autorisations d'utilisation

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

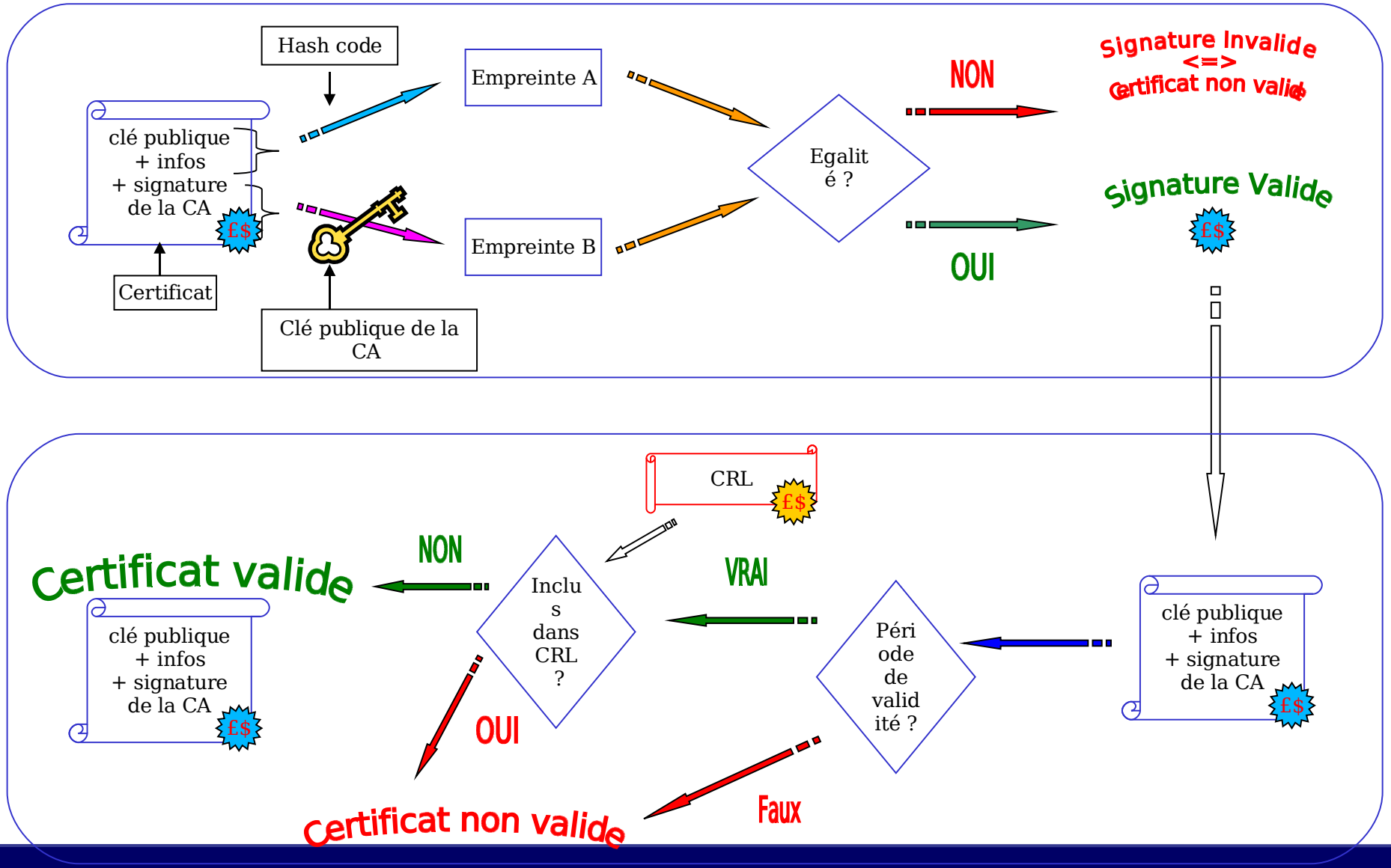
- Signature de la CA

La signature

Signature d'un certificat par la CA émettrice



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
```

Les Autorités de Certification

Enabling Grids for E-science in Europe

- Problématique :
  - Une seule CA par projet => Pas gérable, peu sûr
  - Une CA par partenaire => Problème de mise à l'échelle, peu sûr
- 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

Enabling Grids for E-science in Europe

- 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 (US, Canada, Chine, Taiwan, ...)
- 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

EUGridPMA

Enabling Grids for E-science in Europe

European Policy Management Authority for Grid Authentication

Entité responsable d'établir les obligations et les bonnes pratiques pour les CA délivrant des certificats pour l'authentification sur les GRID.

Son rôle est de créer un domaine de confiance inter-organisation pour permettre l'authentification des personnes et des ressources distribuées.

- Membres : représentant(s) de chaque CA accréditées, représentant(s) des projets utilisateurs
- Actions (réunions tri-annuelles):
  - Etablir les obligations minimales des CA
  - Accréditation des CA : Vérification que les CP/CPS soient en accord avec les obligations minimales demandées, entretien avec représentant(s) des CA
- Etablissement d'une charte

EUGridPMA is a body to establish requirements and best practices for grid identity providers to enable a common trust domain applicable to authentication of end-entities in inter-organisational access to distributed resources

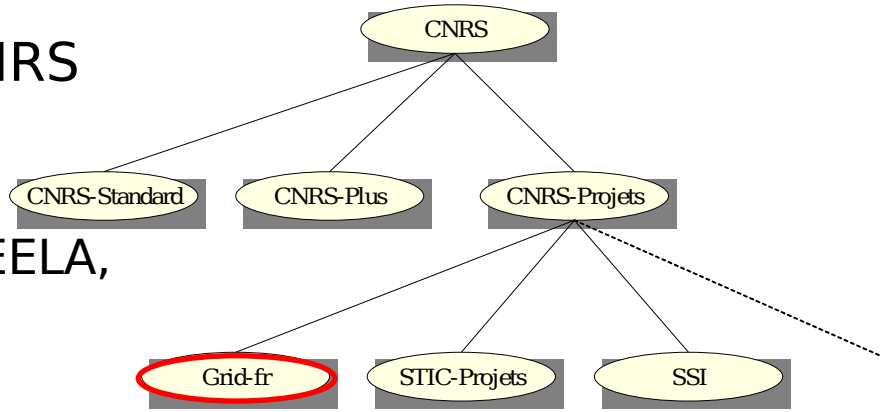
Obligations minimales

- CRL
  - Emettre une CRL dès qu'un certificat est révoqué
  - Validité max un mois, ré-émission 7 jours avant expiration
- Machine CA
  - Dédiée, off-line
  - Protection des clés (clés utilisateurs non conservées)
- 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

Enabling Grids for E-science in Europe

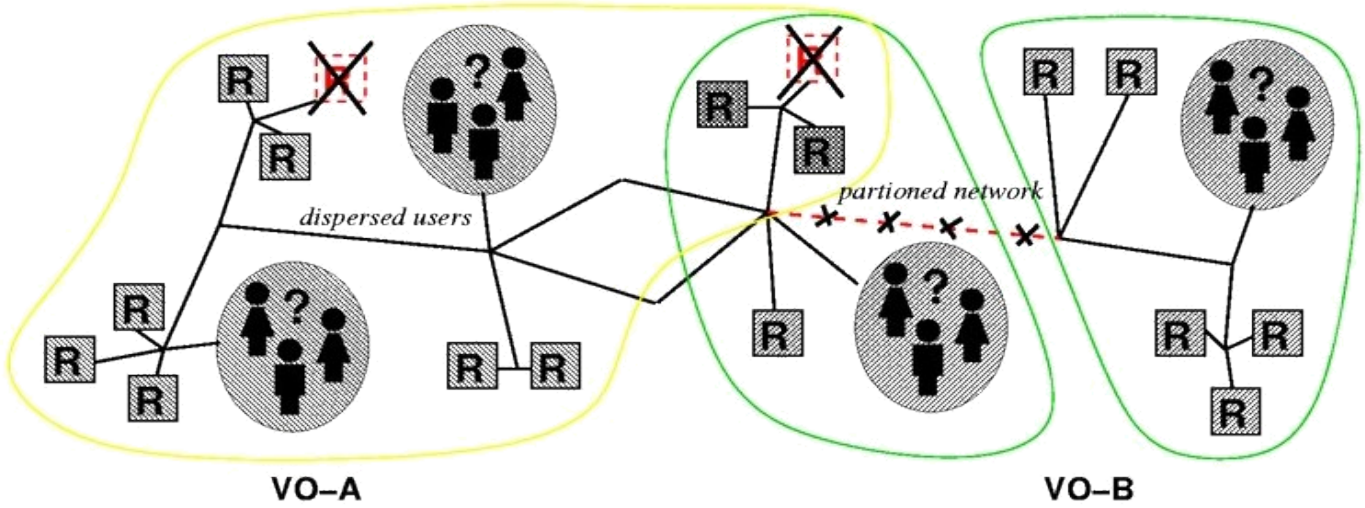
- Spécificités par rapport aux autres sous-CA du CNRS :
  - Sujet des certificats distinctif et unique
  - Possibilité d'avoir des sujets de certificat service :
    - /O=GRID-FR/C=FR/O=CNRS/OU=UREC/CN=ldap/monserveur
  - Certificats émis à d'autres instituts que le CNRS, d'autres pays, ...
  - Extensions 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

GRID-FR. Organisation

- Seulement deux Autorités d'Enregistrement peuvent valider les demandes de création (via un site dédié) et de révocation de certificat
- Dans chaque unité : un représentant local
  - Contacté par email signé à chaque demande de certificat personnel
  - Chargé de vérifier l'identité du demandeur et le bien fondé de sa demande
- Enregistrement de nouvelle organisation ou unité dans la CA
  - Evaluation de la demande
    - Pertinence (projet de GRID, France ou pays sans CA, …)
    - Choix d'un représentant local responsable
  - Etablissement d'un contrat avec le représentant local

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 domaine scientifique, laboratoire, région ou projet
  - Discipline : biomed, alice, lhcb, esr, planck, magic, vo.astro.eu-egee.org, ...
  - Laboratoires, régions : vo.lal.in2p3.fr, vo.grif.fr, seegrid, voce ...
  - Projets : embrace, infngrid, GridPP, auvergrid,...
  - Autre : dteam, ops
- https://cic.in2p3.fr/index.php?id=vo
- Un administrateur (ou plus) par Organisation Virtuelle
  - C'est le gestionnaire des utilisateurs de sa VO
- Base d'acceptation par les sites de la Grille
- Des droits spécifiques peuvent être données au niveau de chaque site par l'administrateur de celui-ci.
  - Interdire l'accès à un groupe d'utilisateurs en fonction de leur sujet de certificat

Les VOMS (1)

- **Les VOMS**
  - La base de données de la VOMS contient l'ensemble des membres avec leur niveau d'autorisation (groupes, rôles, capacités)
  - Un utilisateur peut avoir plusieurs niveaux d'autorisation dans chaque VOMS, faire partie de plusieurs VOMS
  - 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)

Enabling Grids for E-science in Europe

- 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
- Les attributs du proxy sont analysés par chaque site accédés grâce à **LCAS** et **LCMAPS**

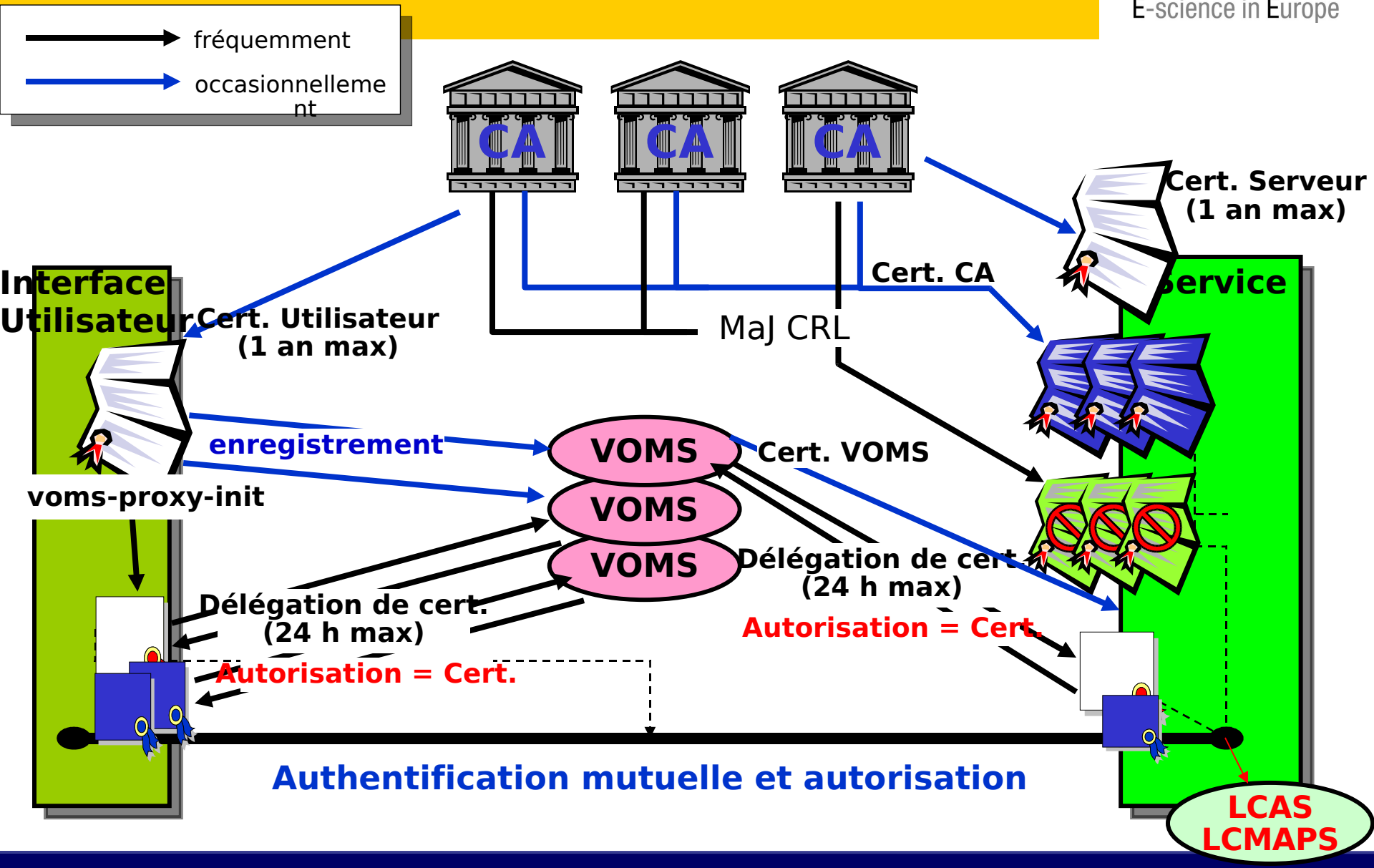
Les VOMS (3)

Enabling Grids for E-science in Europe

- LCAS Vérifie si l'utilisateur est autorisé ou interdit sur ce site
- LCMAPS Fait correspondre le sujet de certificat en fonction des attributs du proxy à un compte utilisateur local au site (UID/GID)
- Les fichier d'autorisations gridmapfile, sur chaque site font correspondre à chaque VOMS/group/rôle un pool de compte ou un compte générique
- Les DPM et LFC utilisent un autre mécanisme (virtual IDs) aux effets similaires

```
"/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



Proxy de courte durée - VOMS

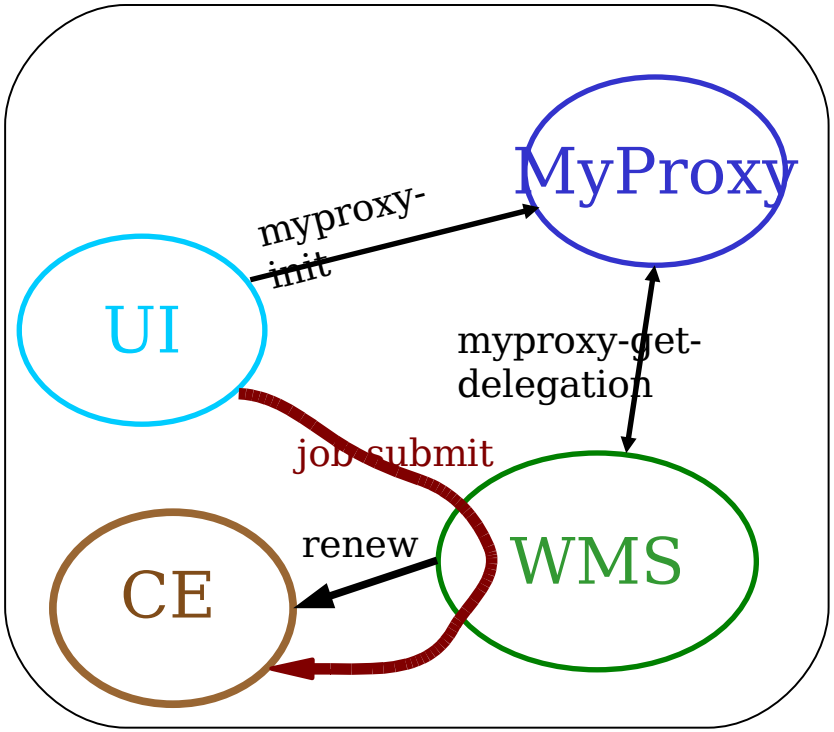
Enabling Grids for E-science in Europe

- Créer un proxy
  - **voms-proxy-init - -voms <vo-name>**
- Créer un proxy en spécifiant un groupe
  - **voms-proxy-init **
    —-voms <vo-name>:/group/subgroup
- 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 -all**
- 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 générer un proxy de longue durée de vie (option --valid HH:MM)
- Cependant, un job peut avoir besoin d'autorisations plus longues

- Le service myproxy permet de créer des autorisatons de longue durée
- Les proxys créés sont conservés par myproxy
- le middleqare effectue le renouvellement des proxys



Proxy de longue durée (2)

Enabling Grids for E-science in Europe

- 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`**
- Obtenir des informations sur un proxy stocké
  - **`myproxy-info -v`**
- Récupérer un proxy stocké
  - **`myproxy-get-delegation`**
- Détruire un proxy stocké
  - **`myproxy-destroy`**

Liens

Enabling Grids for E-science in Europe

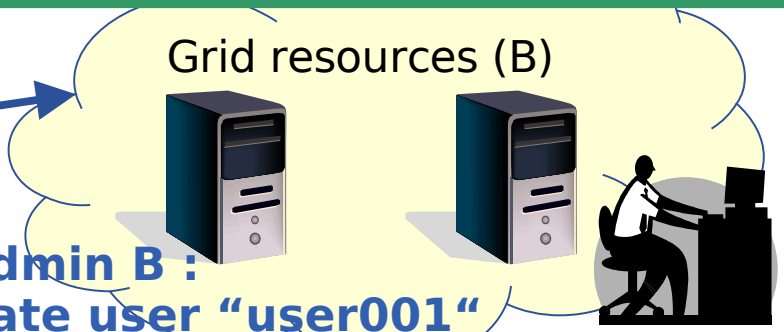
- GSI
  - http://www.globus.org/grid_software/security/
- Autorités de Certification
  - http://gridpma.org/, http://www.eugridpma.org
  - http://igc.services.cnrs.fr/GRID-FR/
- VOMS
  - https://edms.cern.ch/file/572406/1/user-guide.pdf
  - https://grid12.lal.in2p3.fr:8443/voms/astro.vo.eu-egee.org
- MyProxy
  - http://grid.ncsa.uiuc.edu/myproxy/doc.html
- gLite security infrastructure
  - https://edms.cern.ch/document/935451/2

Grids – Conventional grid security

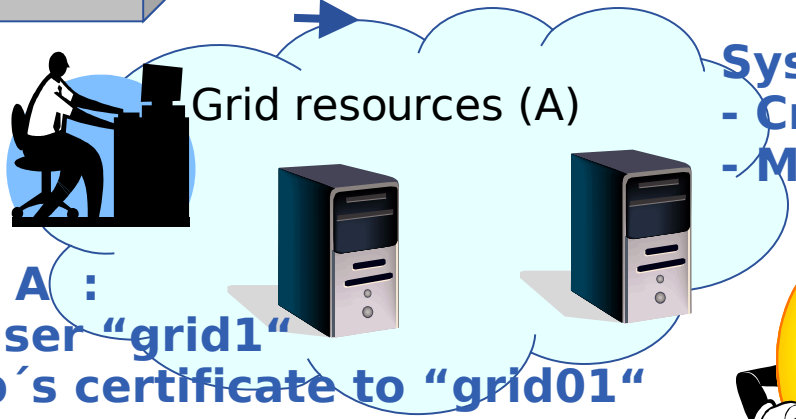
Single sign-on
Delegation through proxy certificat

`grid-proxy-init`

User Interface (UI)



Sysadmin B :
- Create user “user001“
- Map Bob´s certificate to “user001“



Sysadmin A :
- Create user “grid1“
- Map Bob´s certificate to “grid01“

- Manual user “mapping“
- No info about VOs

gLite – Enhanced security