Centre de Calcul
de l'Institut National de Physique Nucléaire
et de Physique des Particules

Autorité de certification GRID-FR (pour l'IN2P3)

Journées LCG-France, juin 2023

Benoit DELAUNAY

Autorité de certification GRID-FR

- GRID-FR, en peu d'histoire.
  - Année de création, année de transfert de la gestion à RENATER ?
- GRID-FR, utilisée par qui ?
  - Combien d'organismes souscripteurs ?
  - Les deux principaux détenteurs des 98% de certificats émis ?
- GRID-FR, en 2023.
  - Plateforme d'hébergement ? Espérance de vie ?
  - Qui ne veut plus/pas s'en occuper ?

Pour résumer…

- L'autorité de certification GRID-FR est hébergée sur une infrastructure matérielle et logicielle vieillissante et sans maintenance.
- RENATER souhaite se désengager de la gestion de GRID-FR.
- L'alternative proposée est le service TCS de GEANT (eScience), conforme IGTF.
- Chaque établissement est responsable d'organiser le basculement de ses certificats sur la nouvelle infrastructure. Le CC-IN2P3 s'est proposé pour l'IN2P3.

Service TCS de GEANT

- Depuis 2020, le CNRS bénéficie à travers RENATER du service d'émission de certificats TCS de GEANT, hébergé sur la plateforme de l'opérateur Sectigo.

  https://services.renater.fr/tcs/

- Plusieurs autorités de certifications proposées pour 5 types d'utilisation.

  https://security.geant.org/trusted-certificate-services/

5 types de certificats proposés

- SSL certificates
  - for authenticating servers and establishing secure sessions with end clients
- Grid certificates
  - for authenticating Grid hosts and services (IGTF compliant)
- Client certificates
  - for identifying individual users and securing email communications
- Code signing certificates
  - for authenticating software distributed over the internet
- Document signing certificates
  - for authenticating documents from Adobe PDF, Microsoft Office, OpenOffice and LibreOffice.

Autorités de certification GEANT eScience

- Deux autorités de certification « IGTF compliant » pour deux usages.

- GEANT eScience SSL CA 4
  - Émission de certificats serveurs

```
issuer= /C=NL/O=GEANT Vereniging/CN=GEANT eScience SSL CA 4
```

- GEANT eScience Personal CA 4
  - Émission de certificats personnel (clients et robots)

```
issuer= /C=NL/O=GEANT Vereniging/CN=GEANT Personal CA 4
```

Non-conformité des certificats CNRS

- Certificate Policy and Certificate Pratice Statement
  - https://wiki.geant.org/display/TCSNT/TCS+Repository

> For certificates issued by the eScience Server CAs all attributes within the certificate subjects contain 7-bit ASCII strings encoded using characters from the IA5STRING subset. For the TCS Server CAs, the attributes shall use an appropriate encoding sufficient to express the names of the Organisation, Organisational Unit, and CommonName, as specified by the CA Operator.

- Le français, les accents et des personnels probablement trop zélés.
  - ST=\xC3\x8Ele-de-France ??? Île-de-France ???

```
subject= /DC=org/DC=terena/DC=tcs/C=FR/ST=\xC3\x8Ele-de-France/O=CNRS/CN=ccdcacli463.in2p3.fr
```

Non-conformité des certificats CNRS

- 2 solutions,
  - supprimer l'attribut ST du DN du certificat (c'est possible, il est optionnel).
  - changer la valeur de l'attribut pour le mettre en conformité avec la règle.

State	ST	(for organisations where it is defined, optional) State or Province in which the organization is based

- Depuis mai 2023, l'attribut STATE est : **ST=Paris**

```
subject= /DC=org/DC=terena/DC=tcs/C=FR/ST=Paris/O=CNRS/CN=ccdcamcli20.in2p3.fr
```

Certificats GEANT eScience SSL

- Certificats serveurs (multi-domaines) maintenant disponibles pour le domaine « in2p3.fr », seul domaine qui nous est délégué.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            b0:16:f0:80:fc:37:8b:52:79:82:90:dc:fc:99:12:a0
    Signature Algorithm: sha384WithRSAEncryption
        Issuer: C=NL, O=GEANT Vereniging, CN=GEANT eScience SSL CA 4
        Validity
            Not Before: Jun  6 00:00:00 2023 GMT
            Not After : Jun  5 23:59:59 2024 GMT
        Subject: DC=org, DC=terena, DC=tcs, C=FR, ST=Paris, O=CNRS, CN=ccdcamcli20.in2p3.fr
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
```

Certificats GEANT eScience Personal

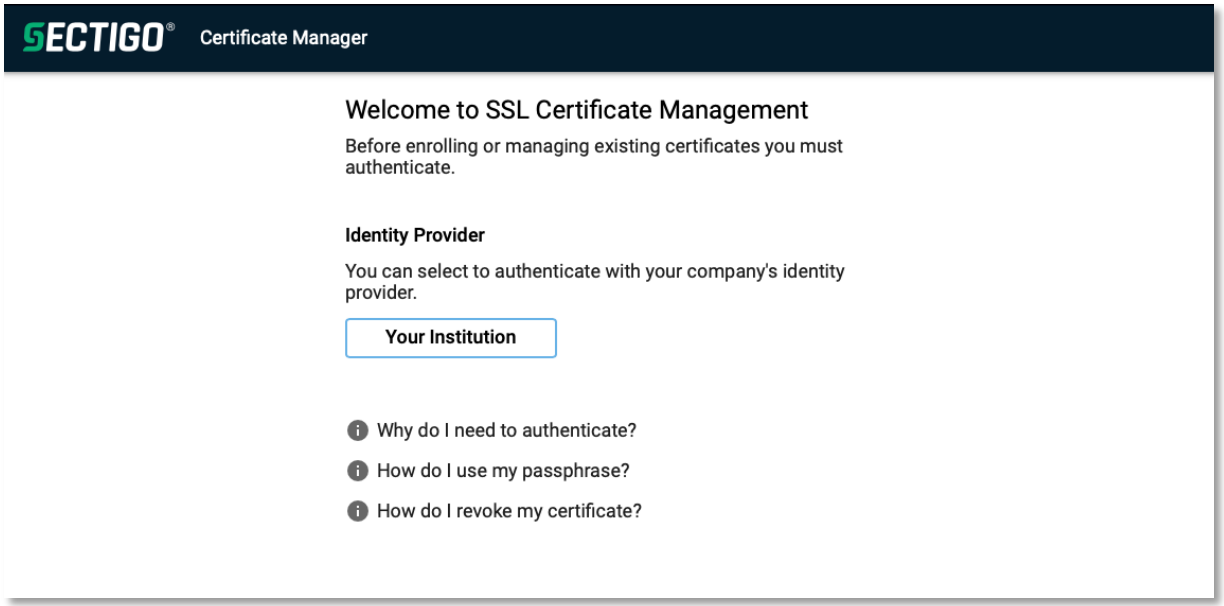
- 2 type de certificats personnels
  - Certificats clients
  - Certificats robots (Classic-Robot Email et MICS-Robot Personal)

- Émission des certificats personnels impossibles à cause d'un problème d'accès au référentiel des agents CNRS (seul problème ?).
  - Discussion en cours avec GEANT, RENATER et la DSI du CNRS.

Émission de certificats serveurs IN2P3

- Formulaire de demande de certificat serveur GEANT (CNRS)
  - https://cert-manager.com/customer/Renater/ssl/in2p3-geant-server
- Formulaire de demande de certificat serveur GEANT eScience (grille de calcul EGI/WLCG)
  - https://cert-manager.com/customer/Renater/ssl/in2p3-geant-escience-server

Démo


SECTIGO
Certificate Manager
Welcome to SSL Certificate Management
Before enrolling or managing existing certificates you must authenticate.
Identity Provider
You can select to authenticate with your company's identity provider.
Your Institution
Why do I need to authenticate?
How do I use my passphrase?
How do I revoke my certificate?

Merci ! Questions ?