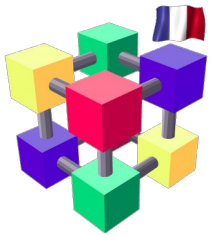
Vers les tokens : état des lieux

David Bouvet
Journées LCG-France, IPHC - 7-9 juin 2022



X509 → tokens

Pourquoi ?

- Volonté de suivre ce qu'il se passe dans l'industrie, mais aussi dans le monde académique
  - ne pas s'isoler, rester en lien avec les communautés
- Alternatives plus « conviviales »

X509 → fédérations d'identité et tokens

WLCG Authorization WG créé en 2017

https://twiki.cern.ch/twiki/bin/view/LCG/WLCGAuthorizationWG

WG for Transition to Tokens and Globus Retirement créé en 2021

https://twiki.cern.ch/twiki/bin/view/LCG/WLCGTokensGlobusWG

→ coordination opérationnelle

X509 → tokens

Fin du support Globus par OSG

- HTTPS pour les transferts
- SciTokens, HTTPS et OAuth2 pour AAI

  → accélération du processus d'abandon par WLCG

Calendrier pour la transition vers les WLCG tokens

https://docs.google.com/document/d/11fcZU8fEsfjDiSkjh95nVr4tNXLPCA_xwr2SwriBpiw/edit#heading=h.s0j7quda1urv

- VOMS → INDIGO IAM
- X509 → JSON Web Tokens
  - compatibilité OSG ?
    - bibliothèques compatibles SciTokens et WLCG JW tokens

EGI

- VOMS → EGI CheckIn
- X509 → AARC (Authentication and Authorisation for Research and Collaboration) Tokens

X509 → tokens

Transferts ✔

- Géré par DOMA TPC WG
- Remplacement de GridFTP par HTTPS / WebDAV ou XRootD
  - compatibles X509 et tokens

Service IAM ✔

- IAM VOMS endpoint :
  - ATLAS et CMS : en production depuis fév. 2022
    - fichiers LSC fournis en sept. 2021
  - ALICE et LHCb : moins urgent et en cours de réalisation
- ATLAS, CMS et SAM ETF
  - tokens possibles pour soumettre des jobs
    - X509 toujours pour gestion données
- Service pas encore en HA
- VOMS-Admin API → REST SCIM API
  - améliorations/fonctionnalités à ajouter

X509 → tokens

Jobs ✔

- ARC-CE
  - via interface REST
  - pas de fin de support X509 programmée
- HTCondor-CE
  - série 9.0.x (LTS) : support de X509 jsq'au 01/02/2023
  - version 9.3.0+ : ~~support X509~~

    → **tickets en cours pour activation support des tokens**
- Durée de vie tokens
  - jobs pilotes : 4 jours pour le moment, idéalement 6 h
    Réduction après :
    - développements nécessaires pour pouvoir configurer la durée de vie
    - IAM en HA + confiance dans le service

Tokens : services

MyProxy ✔

- 2 solutions pour son remplacement :
  - HashiCorp Vault + *htgettoken* → FNAL
    - en cours de test au CERN
  - MyToken → EOSC Synergy infrastructure
    - permet des restrictions sur les tokens et les worflows

DIRAC ✔

- Bientôt compatible tokens (WLCG et AARC)
- Développement pour l'implémentation de l'accès aux données et gestion des tokens longs

Rucio ✔

- OK pour token WLCG
- AARC ?

FTS ✔

- OK pour token WLCG
- AARC ?

Tokens : stockage

Dcache ✔

- OK pour token WLCG
- AARC à faire

STORM ✔

- Partie WebDAV → OK pour WLCG, à faire pour AARC
- Spécifications en cours pour Tape REST API

EOS ✔

- OK pour token WLCG (utilisation bibliothèques XRootD)
- Travail en cours pour être compatible avec les tests WLCG JWT

XRootD ✔

- OK pour token WLCG

Accès au stockage

- Granularité permissions semble suffisante avec champs `wlcg.groups`
- GFAL2 2.20.5 dans epel
  - support des SE-token pour toutes les opérations
- Tokens de courte durée requis à terme pour atteindre le niveau de sécurité attendu

X509 → tokens

Encore beaucoup de travail à faire

- Difficile de prendre en compte tous les cas d'usage
  - définition d'un « trusted token issuer » ?
  - interopérabilité avec autres communautés (tokens non JWT)
    → prochaine version JWT sera moins centrée sur WLCG
  - plus d'accès simple aux informations de l'utilisateur
    - génération gridmap files
    - traçabilité/blocage
  - token pour payload
  - quelle granularité : 1 token pour toutes les actions ou 1 token par action ?
- Rafraîchissement token
- Révocation
- …

→ WLCG AuthZ WG