CILogon

SCITOKENS

Jim Basney
jbasney@ncsa.lllinois.edu

INTERNET2
2022
TECHNOLOGY
exchange

CILogon

Tokens for Science

OpenID Connect (OIDC) ID Tokens (e.g., SCiMMA)
containing user attributes and group memberships
from the research community (via COmanage)
and from the researcher's home institution (via InCommon)

SciTokens (e.g., LIGO)
containing authorization scope values
determined by per client/subscriber policy

WLCG Tokens (e.g., Fermilab)
support for wlcg.groups and storage.*|compute.* scopes

GA4GH Passports (e.g., Australian BioCommons)
support for AffiliationAndRole, AcceptedTermsAndPolicies, ResearcherStatus, ControlledAccessGrants, and LinkedIdentities

https://www.cilogon.org/jwt

Capability-based authorization for distributed scientific computing

- Using the OAuth and JWT standards for distributed authorization
- Using well-supported security libraries/frameworks
- Implementing the Principle of Least Privilege
- Migrate from identity-based authorization (grid-mapfile) to capability-based authorization (audience & scope)

https://scitokens.org/

Open Source

Python library	https://github.com/scitokens/scitokens
C++ library	https://github.com/scitokens/scitokens-cpp
Java client and server	https://github.com/scitokens/scitokens-java
HTCondor CredMon	https://github.com/htcondor/scitokens-credmon
SciTokens SSH	https://github.com/XSEDE/oauth-ssh/tree/master/server#scitokens
CVMFS	https://github.com/cvmfs-contrib/cvmfs-x509-helper
dCache	https://github.com/dCache/dcache
NGINX	https://github.com/scitokens/nginx-scitokens
XRootD	https://github.com/xrootd/xrootd/tree/master/src/XrdSciTokens

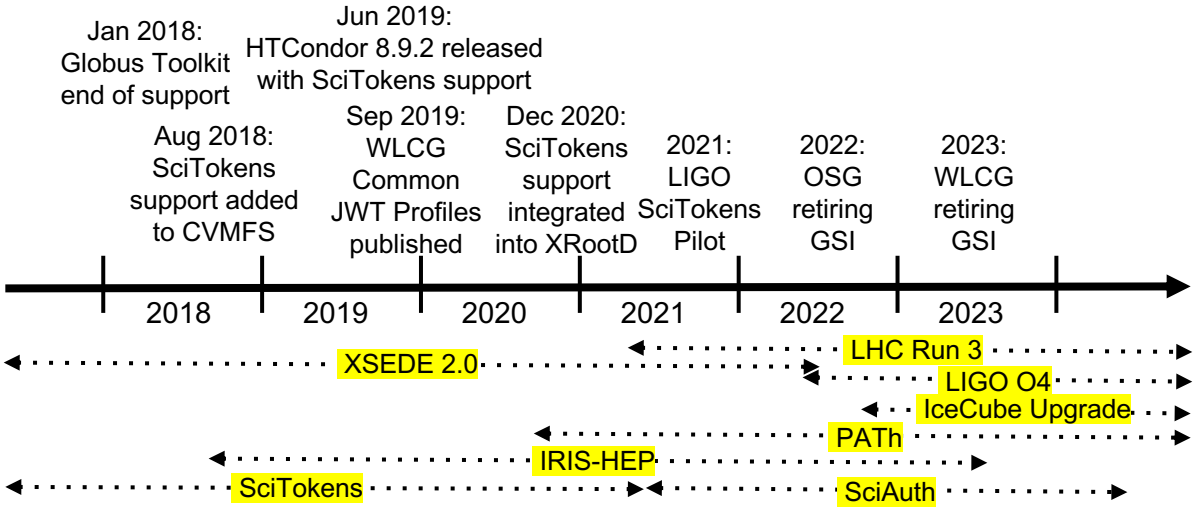
https://scitokens.org/

SciAuth: Deploying Interoperable and Usable Authorization Tokens to Enable Scientific Collaborations

- Transformation underway for authentication and authorization in NSF cyberinfrastructure: from X.509 user certificates to JSON Web Tokens (JWTs)
  - Building on prior work from SciTokens
- An opportunity to realize security benefits:
  - Apply the principle of least privilege
  - Improved support for federated identities (InCommon)
  - Improved support for attribute, role, and capability-based authorization
  - Reduce reliance on coarse-grained identity-based authorization (impersonation)
  - Build on well-supported, widely-used JWT libraries
- With coordination across science projects (LIGO, OSG, WLCG, etc.)
  - For interoperability across infrastructures
  - With common approaches to integration with science software and workflows
  - Working together to maintain/improve reliability/security throughout the transition and beyond

https://sciauth.org/

SciAuth: Timeline



SciTokens for LIGO

- Dedicated https://cilogon.org/ligo token issuer
- Migrating to https://cilogon.org/igwn soon
- vault.ligo.org server for token management
- HTCondor token management for workflows
- Target applications:
  - OSDF/CVMFS/XRootD, GWDataFind, DQSegDB, GraceDB

LIGO Scientific Collaboration

Authorization Policies

scope(s)	group(s)
read:/frames gwdatafind.read dqsegdb.read gracedb.read	Communities:LSCVirgoLIGOGroupMembers gw-astronomy:KAGRA-LIGO:members
write:/frames	Services:XRootD:SciTokens:write-frames:authorized
dqsegdb.create	Communities:LVC:SegDB:SegDBWriter

LIGO Scientific Collaboration

Current Status

- CVMFS HTCondor access in operation
- GraceDB & GWDataFind support implemented and being deployed
- DQSegDB support under development
- Robot support under development
- Bi-weekly coordination calls to prepare for tokens in next LIGO Observing Run (O4) - March 2023

Current Challenges

- Issuer key rotation
- Refresh token rotation
- Various use cases for token exchange
- Policies for dynamic client registration
- High Availability, scalability, and token lifetimes

INTERNET2

2022 TECHNOLOGY exchange

This material is based upon work supported by the National Science Foundation under Grant No. 2114989. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

INTERNET2