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
• 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/
<table>
<thead>
<tr>
<th></th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Python library</td>
<td><a href="https://github.com/scitokens/scitokens">https://github.com/scitokens/scitokens</a></td>
</tr>
<tr>
<td>C++ library</td>
<td><a href="https://github.com/scitokens/scitokens-cpp">https://github.com/scitokens/scitokens-cpp</a></td>
</tr>
<tr>
<td>Java client and server</td>
<td><a href="https://github.com/scitokens/scitokens-java">https://github.com/scitokens/scitokens-java</a></td>
</tr>
<tr>
<td>HTCondor CredMon</td>
<td><a href="https://github.com/htcondor/scitokens-credmon">https://github.com/htcondor/scitokens-credmon</a></td>
</tr>
<tr>
<td>SciTokens SSH</td>
<td><a href="https://github.com/XSEDE/oauth-ssh/tree/master/server#scitokens">https://github.com/XSEDE/oauth-ssh/tree/master/server#scitokens</a></td>
</tr>
<tr>
<td>CVMFS</td>
<td><a href="https://github.com/cvmfs-contrib/cvmfs-x509-helper">https://github.com/cvmfs-contrib/cvmfs-x509-helper</a></td>
</tr>
<tr>
<td>dCache</td>
<td><a href="https://github.com/dCache/dcache">https://github.com/dCache/dcache</a></td>
</tr>
<tr>
<td>NGINX</td>
<td><a href="https://github.com/scitokens/nginx-scitokens">https://github.com/scitokens/nginx-scitokens</a></td>
</tr>
<tr>
<td>XRootD</td>
<td><a href="https://github.com/xrootd/xrootd/tree/master/src/XrdSciTokens">https://github.com/xrootd/xrootd/tree/master/src/XrdSciTokens</a></td>
</tr>
</tbody>
</table>

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

Jan 2018: Globus Toolkit end of support

Aug 2018: SciTokens support added to CVMFS

Jun 2019: HTCondor 8.9.2 released with SciTokens support

Sep 2019: WLCG Common JWT Profiles published

Dec 2020: SciTokens support integrated into XRootD

2021: LIGO SciTokens Pilot

2022: OSG retiring GSI

2023: WLCG retiring GSI

2023:

2022:

2021:

2020:

2019:

2018:

Aug 2018: SciTokens support added to CVMFS

Jun 2019: HTCondor 8.9.2 released with SciTokens support

Sep 2019: WLCG Common JWT Profiles published

Dec 2020: SciTokens support integrated into XRootD

2021: LIGO SciTokens Pilot

2022: OSG retiring GSI

2023: WLCG retiring GSI

2023:

2022:

2021:

2020:

2019:

2018:

Aug 2018: SciTokens support added to CVMFS

Jun 2019: HTCondor 8.9.2 released with SciTokens support

Sep 2019: WLCG Common JWT Profiles published

Dec 2020: SciTokens support integrated into XRootD

2021: LIGO SciTokens Pilot

2022: OSG retiring GSI

2023: WLCG retiring GSI

2023:

2022:

2021:

2020:

2019:

2018:

Aug 2018: SciTokens support added to CVMFS

Jun 2019: HTCondor 8.9.2 released with SciTokens support

Sep 2019: WLCG Common JWT Profiles published

Dec 2020: SciTokens support integrated into XRootD

2021: LIGO SciTokens Pilot

2022: OSG retiring GSI

2023: WLCG retiring GSI

2023:

2022:

2021:

2020:

2019:

2018:

Aug 2018: SciTokens support added to CVMFS

Jun 2019: HTCondor 8.9.2 released with SciTokens support

Sep 2019: WLCG Common JWT Profiles published

Dec 2020: SciTokens support integrated into XRootD

2021: LIGO SciTokens Pilot

2022: OSG retiring GSI

2023: WLCG retiring GSI

2023:
• 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
<table>
<thead>
<tr>
<th>scope(s)</th>
<th>group(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>read:/frames</td>
<td>Communities: LSCVirgoLIGOGroupMembers</td>
</tr>
<tr>
<td>gwdatafind.read</td>
<td>gw-astronomy: KAGRA-LIGO:members</td>
</tr>
<tr>
<td>dqsegdb.read</td>
<td></td>
</tr>
<tr>
<td>gracedb.read</td>
<td></td>
</tr>
<tr>
<td>write:/frames</td>
<td>Services: XRootD:SciTokens:write-frames:authorized</td>
</tr>
<tr>
<td>dqsegdb.create</td>
<td>Communities: LVC:SegDB:SegDBWriter</td>
</tr>
</tbody>
</table>
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
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.