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

Jim Basney <jbasney@ncsa.illinois.edu>
Brian Bockelman <bbockelman@morgridge.org>
Derek Weitzel <dweitzel@unl.edu>

2021 NSF Cybersecurity Summit

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.
Why SciAuth?

- 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
Capability-based Authorization for Distributed Science
Or, “How I learned to stop worrying about identity”

- **Authorization** - determining access rights or privileges to a given resource - is something we do in everyday life:
  - My ID card gets me into my office building.
  - My passport allows me to get into a new country (if we ever get to travel again!).
  - A baseball ticket gets me access into a baseball game.
  - The Zoom URL got everyone into this meeting!

- I think of it as a function that takes some inputs and returns some number of privileges.
- Unfortunately, in computing, we too often intermix the concept of authorization with **authentication**!

\[ A_{Z}(\ldots) \rightarrow P_1, P_2, \ldots, P_N \]
Not every scheme requires auth’n as inputs to auth’z.

Authentication: establishing an identity for a remote entity.

Potentially, username and password is the most familiar authorization scheme:

- A remote entity provides a username/password (credentials) to authenticate to an identity.
- This identity is mapped to a list of authorized access rights.

Note you can have traceability even if you didn’t use authentication for authorization!

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Credentials</th>
<th>Authentication</th>
<th>Authorization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gmail login</td>
<td>Password, 2FA</td>
<td>Username</td>
<td>Access to your inbox</td>
</tr>
<tr>
<td>Office building</td>
<td>ID card</td>
<td>Identity in HR database</td>
<td>Elevators</td>
</tr>
<tr>
<td>access</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>International</td>
<td>Passport</td>
<td>Identity</td>
<td>Enter Switzerland</td>
</tr>
<tr>
<td>Travel</td>
<td></td>
<td>according to US Government</td>
<td></td>
</tr>
<tr>
<td>Baseball Game</td>
<td>Ticket</td>
<td>NONE!</td>
<td>Sit in section 4, seat 34B</td>
</tr>
<tr>
<td>Webinar</td>
<td>Zoom URL</td>
<td>NONE!</td>
<td>Attend this wonderful summit!</td>
</tr>
</tbody>
</table>
Distributed Scientific Computing

Often in distributed scientific computing, the resource provider has a relationship with an organization, not the individual:

- In the OSG, the organization requests resources from sites and these join a global pool.
- When computing on AWS for a collaboration, someone centrally handles the billing for the resources launched. Not every user sends their credit card to Amazon.
- In XSEDE community accounts, the resource provider interacts with the community and the community interacts with the user.
- **Counter-example:** for traditional XRAC allocations, the user gets an individual account on the resource.
Historically, the OSG used client X.509 certificates (and some related extensions for group attributes and impersonation) to authenticate users and identity mapping as an authorization scheme:

- The X.509 certificate established a **global identity**.
- The site established an **identity mapping** function to a local identity (e.g., a Unix account).
- The client is **authorized** for any privileges given to the local identity.

Problems?

- No fine grained authorization. Your “power of attorney” travels to every remote host on the planet.
- Resource doesn’t have the relationship with the user; the actual authorization decisions belong to the organization **within** their space allocation.
Scientific Computing and Tokens

A capability is an (unforgeable) token that authorizes a given action on an object.

- Your house key is a capability: anyone with the key is authorized to enter the door. No need to establish an identity to use a house key!
- The capability says “What you can do, not Who you are!”

Within our community, we have built on top of the JSON Web Token (JWT) standard to allow distributed token verification and a set of agreed-upon capabilities. See doi:10.5281/zenodo.3460258

Scientific Computing and Tokens

Each token has a ‘issuer’ (maps to the scientific organization) and a set of fine-grained capabilities.

- Capabilities are evaluated with respect to the issuer’s authorization.
- Remote resources need to map the issuer to resources. Do not need to know the individual users.
- Especially for file access, we can go fine-grained down to individual files.

```
{
    'wlcg-ver': '1.0',
    'sub': '27234843-fedf-42c8-bb81-a1695b0d7c28',
    'aud': 'https://wlcg.cern.ch/jwt/v1/any',
    'nbf': 1618763119,
    'scope': 'openid offine_access storage.read://
              storage.modify:// wlcg',
    'iss': 'https://wlcg-cmssw.cern.infn.it/',
    'exp': 1618766719,
    'iat': 1618763119,
    'jti': 'ff78bede-28a8-4997-85d6-b89004a2e903',
    'client_id': 'b68d97d4b-621d-4f7f-974c-bc5a8e3be48'
}
```

Read / write within the issuer’s namespace at a storage endpoint
Demonstrated a capabilities-based authorization infrastructure for distributed scientific computing

Using the OAuth and JWT standards for distributed authorization

Implementing the Principle of Least Privilege

Visit https://scitokens.org/ for specifications, publications

Visit https://github.com/scitokens for open source implementations
Using Standards

- RFC 6749: OAuth 2.0 Authorization Framework
  - token request, consent, refresh
- RFC 7519: JSON Web Token (JWT)
  - self-describing tokens, distributed validation
- RFC 8414: OAuth 2.0 Authorization Server Metadata
  - token signing keys, policies, endpoint URLs
- RFC 8693: OAuth 2.0 Token Exchange
  - token delegation, drop privileges
- JSON Web Token (JWT) Profile for OAuth 2.0 Access Tokens
  - authorization claims (scope, aud), metadata for validation
WLCG Common JWT Profiles

● Defines profiles for Group Based Authorization (wlcg.groups) and Capability Based Authorization (scope)

● Use cases:
  a. Identity Token with Groups
  b. Access Token with Groups
  c. Access Token with Authorization Scopes

● SciTokens supports and helped define use case (c)

https://doi.org/10.5281/zenodo.3460257
https://github.com/WLCG-AuthZ-WG
SciAuth Approach

Science Drivers
- FNAL (HEP)
- IceCube (HEP)
- LIGO (Astro)
- OSG (HTC)
- WLCG (LHC)
- XSEDE (HPC)

Outreach, Training, Workforce
- AEGIS
- CI CoE Pilot
- CI Logon / InCommon
- REFEDS
- TAGPMA
- Trusted CI

SciAuth
- Training Modules
- Fellows Projects
- Papers & Docs

Software Cyberinfrastructure
- CVMFS
- Gateways
- HTCondor
- Jupyter
- XRootD
What is the timeline?

Jan 2018: Globus Toolkit end of support

Aug 2018: SciTokens support added to CVMFS

Sep 2019: WLCG Common JWT Profiles published

Dec 2020: SciTokens support integrated into XRootD

Jun 2019: HTCondor 8.9.2 released with SciTokens support

2021:

Jun 2019: HTCondor 8.9.2 released with SciTokens support

Aug 2018: SciTokens support added to CVMFS

Dec 2020: SciTokens support integrated into XRootD

2022:

2023:

Jan 2023: OSG retiring GSI

2023:

Dec 2020: SciTokens support integrated into XRootD

Aug 2018: SciTokens support added to CVMFS

2021:

2022:

2023:

Jan 2018: Globus Toolkit end of support

Aug 2018: SciTokens support added to CVMFS

Sep 2019: WLCG Common JWT Profiles published

Dec 2020: SciTokens support integrated into XRootD

Jun 2019: HTCondor 8.9.2 released with SciTokens support

2021:

Jun 2019: HTCondor 8.9.2 released with SciTokens support

Aug 2018: SciTokens support added to CVMFS

Dec 2020: SciTokens support integrated into XRootD

2022:

2023:

Jan 2023: OSG retiring GSI

2023:

Dec 2020: SciTokens support integrated into XRootD

Aug 2018: SciTokens support added to CVMFS

2021:

2022:

2023:

Jan 2018: Globus Toolkit end of support

Aug 2018: SciTokens support added to CVMFS

Sep 2019: WLCG Common JWT Profiles published

Dec 2020: SciTokens support integrated into XRootD

Jun 2019: HTCondor 8.9.2 released with SciTokens support

2021:

Jun 2019: HTCondor 8.9.2 released with SciTokens support

Aug 2018: SciTokens support added to CVMFS

Dec 2020: SciTokens support integrated into XRootD

2022:

2023:

Jan 2023: OSG retiring GSI

2023:

Dec 2020: SciTokens support integrated into XRootD

Aug 2018: SciTokens support added to CVMFS

2021:

2022:

2023:

Jan 2018: Globus Toolkit end of support

Aug 2018: SciTokens support added to CVMFS

Sep 2019: WLCG Common JWT Profiles published

Dec 2020: SciTokens support integrated into XRootD

Jun 2019: HTCondor 8.9.2 released with SciTokens support

2021:

Jun 2019: HTCondor 8.9.2 released with SciTokens support

Aug 2018: SciTokens support added to CVMFS

Dec 2020: SciTokens support integrated into XRootD

2022:

2023:

Jan 2023: OSG retiring GSI

2023:

Dec 2020: SciTokens support integrated into XRootD

Aug 2018: SciTokens support added to CVMFS

2021:

2022:

2023:

Jan 2018: Globus Toolkit end of support

Aug 2018: SciTokens support added to CVMFS

Sep 2019: WLCG Common JWT Profiles published

Dec 2020: SciTokens support integrated into XRootD

Jun 2019: HTCondor 8.9.2 released with SciTokens support

2021:

Jun 2019: HTCondor 8.9.2 released with SciTokens support

Aug 2018: SciTokens support added to CVMFS

Dec 2020: SciTokens support integrated into XRootD

2022:

2023:

Jan 2023: OSG retiring GSI

2023:

Dec 2020: SciTokens support integrated into XRootD

Aug 2018: SciTokens support added to CVMFS

2021:

2022:

2023:

Jan 2018: Globus Toolkit end of support

Aug 2018: SciTokens support added to CVMFS

Sep 2019: WLCG Common JWT Profiles published

Dec 2020: SciTokens support integrated into XRootD

Jun 2019: HTCondor 8.9.2 released with SciTokens support

2021:

Jun 2019: HTCondor 8.9.2 released with SciTokens support

Aug 2018: SciTokens support added to CVMFS

Dec 2020: SciTokens support integrated into XRootD

2022:

2023:

Jan 2023: OSG retiring GSI

2023:

Dec 2020: SciTokens support integrated into XRootD

Aug 2018: SciTokens support added to CVMFS

2021:

2022:

2023:

Jan 2018: Globus Toolkit end of support

Aug 2018: SciTokens support added to CVMFS

Sep 2019: WLCG Common JWT Profiles published

Dec 2020: SciTokens support integrated into XRootD

Jun 2019: HTCondor 8.9.2 released with SciTokens support

2021:

Jun 2019: HTCondor 8.9.2 released with SciTokens support

Aug 2018: SciTokens support added to CVMFS

Dec 2020: SciTokens support integrated into XRootD

2022:

2023:

Jan 2023: OSG retiring GSI

2023:

Dec 2020: SciTokens support integrated into XRootD

Aug 2018: SciTokens support added to CVMFS

2021:

2022:

2023:

Jan 2018: Globus Toolkit end of support

Aug 2018: SciTokens support added to CVMFS

Sep 2019: WLCG Common JWT Profiles published

Dec 2020: SciTokens support integrated into XRootD

Jun 2019: HTCondor 8.9.2 released with SciTokens support

2021:

Jun 2019: HTCondor 8.9.2 released with SciTokens support

Aug 2018: SciTokens support added to CVMFS

Dec 2020: SciTokens support integrated into XRootD

2022:

2023:

Jan 2023: OSG retiring GSI

2023:

Dec 2020: SciTokens support integrated into XRootD

Aug 2018: SciTokens support added to CVMFS

2021:

2022:

2023:
SciAuth Activities

Areas:
● Coordination, Outreach, and Training
● Security
● Software (demonstrations, integrations)
● Standards (JWT profiles, interop)
● Workforce Development (student fellows)

Tasks in Security Area:
● Threat Model
● Operational guidelines for token issuers
● Assessment of JWT implementations
● Token issuer peer reviews
● Tabletop exercises
  ○ Refresh token compromise
  ○ Token issuer compromise
  ○ Submit node compromise
  ○ Identity provider compromise (SIRTFI)

SciAuth is about supporting the community's transition to tokens
Not about developing new software or capabilities
Threat Model

Science Asset: Embargoed/Internal Data

Lost Effort Reproducing Data
Loss of non-reproducible data
Inaccessible or Lost Data
Corrupted Data
Exposed Data
Credential Exposure

Concerns

Consequences

Incorrect Science Results
Reputation Loss
Legal Action

Avenues of Attack

User Grants Too Much Access Scope
Malicious Client Obtains Authorization

https://www.trustedci.org/oscrp
## Threat Model

<table>
<thead>
<tr>
<th>Threats</th>
<th>Mitigations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credential Exposure</td>
<td>Short lifetimes for access tokens</td>
</tr>
<tr>
<td></td>
<td>Encrypted transit</td>
</tr>
<tr>
<td></td>
<td>Well-protected refresh tokens</td>
</tr>
<tr>
<td></td>
<td>Token revocation</td>
</tr>
<tr>
<td>Granting too much access</td>
<td>Least-privilege delegation</td>
</tr>
<tr>
<td></td>
<td>Token exchange to drop privileges</td>
</tr>
<tr>
<td>Malicious client</td>
<td>Client registration and vetting</td>
</tr>
<tr>
<td></td>
<td>Client revocation</td>
</tr>
<tr>
<td></td>
<td>Per-client policies</td>
</tr>
<tr>
<td>Issuer compromise</td>
<td>Key revocation via Authorization Server Metadata</td>
</tr>
</tbody>
</table>

References:
- RFC 6819 (OAuth 2.0 Threat Model and Security Considerations)
- RFC 8725 (JSON Web Token Best Current Practices)
Webinars & Workshops

Recent Webinars (https://www.trustedci.org/webinars):

- Jul '21: A capability-based authorization infrastructure for distributed High Throughput Computing in Open Science Grid

Upcoming Events:

- Oct 14-15 OSG Token Transition Workshop
  https://sciauth.org/2021/10/14/OSG.html
- Oct 18 Summit Workshop on Token-Based Authentication and Authorization
  https://sciauth.org/workshop/2021/
Workforce Development - SciAuth Student Fellows

- Now accepting applications!
- Seeking students who:
  - are interested in tokens!
  - are currently enrolled at an accredited U.S. higher education institution. Both graduate and undergraduate students are eligible.
  - will reside in the United States during the 12 week fellowship period (schedule to be determined by fellow and mentor).
- Travel is not required. All fellows program activities are conducted online.
- Fellows each receive a $1,000 stipend ($333.33 per month for 3 months) to support their research.
- For more info: https://sciauth.org/fellows
Thanks!

Visit
https://sciauth.org/
for more info.

Contact:
bbockelman@morgridge.org
dweitzel@unl.edu
jbasney@illinois.edu