From Identity-Based Authorization to Capabilities: SciTokens, JWTs, and OAuth

Jim Basney
jbasney@ncsa.illinois.edu
OSG All Hands Meeting
3 March 2021
Goals for a dHTC Authorization System

- Enable access to dHTC for the advancement of open science!
- Implement appropriate resource/data access policies
- Ease of use
- Manageability
- Distributed/Decentralized
Authentication & Authorization Standards

- X.509: Certificates
  - Grid Security Infrastructure (GSI)
  - Virtual Organization Membership Service (VOMS)
- SAML: Security Assertion Markup Language
  - Using XML
  - Single Sign-on for Higher Education: eduGAIN / InCommon / Shibboleth
- JWT: JSON Web Tokens
  - Using JavaScript Object Notation (JSON)
  - Pronounced "jot"
  - Digitally signed, self-describing security tokens
- OAuth: Authorization Framework
  - Optionally using JWTs
  - Tokens for limited access to resources
- OIDC: OpenID Connect
  - An identity layer on top of OAuth
  - Using JWTs
X.509
SAML
## Credentials for Authentication / Authorization

<table>
<thead>
<tr>
<th>Credential Issuer</th>
<th>X.509</th>
<th>SAML</th>
<th>OIDC</th>
<th>OAuth / JWT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Authority</td>
<td>Identity Provider</td>
<td>OpenID Provider</td>
<td>Authorization Server</td>
<td></td>
</tr>
<tr>
<td>Certificate Verifier</td>
<td>Relying Party</td>
<td>Service Provider</td>
<td>Relying Party</td>
<td>Resource Server</td>
</tr>
<tr>
<td>Credential</td>
<td>Certificate</td>
<td>Assertion</td>
<td>ID Token</td>
<td>Access Token</td>
</tr>
<tr>
<td>Language</td>
<td>ASN.1</td>
<td>XML</td>
<td>JSON</td>
<td>JSON</td>
</tr>
<tr>
<td>Credential Contents</td>
<td>Distinguished Names</td>
<td>Attributes</td>
<td>Claims</td>
<td>Claims</td>
</tr>
<tr>
<td></td>
<td>/ Fully Qualified</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Attribute Names</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Identifier</td>
<td>Subject DN</td>
<td>NameID /</td>
<td>Subject Identifier (sub) Claim</td>
<td>Subject (sub) Claim</td>
</tr>
<tr>
<td></td>
<td></td>
<td>eduPersonPrincipalName</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Managing Trust</td>
<td>CA Certificate Bundle</td>
<td>SAML Metadata</td>
<td>OpenID Provider Metadata</td>
<td>Authorization Server Metadata</td>
</tr>
</tbody>
</table>
# Authorization / Access Control

<table>
<thead>
<tr>
<th></th>
<th>X.509</th>
<th>SAML</th>
<th>OIDC</th>
<th>OAuth</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Identity-based</strong></td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>User identifiers and access control lists</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Attribute-based</strong></td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Access policies based on user attributes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Role-based</strong></td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Access controls based on group memberships and roles</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Capability-based</strong></td>
<td>YES</td>
<td></td>
<td></td>
<td>YES ⭐</td>
</tr>
<tr>
<td>Tokens allow actions on resources</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
OIDC JWT Demo

Log on to https://demo.cilogon.org/ with your campus identity provider or use your GitHub, Google, or ORCID account.
OIDC JWT Demo

Paste the ID Token and Public Key into https://jwt.io/ to verify it.
Least Privilege Authorization

- Good security practice: grant only those privileges that are required
  - for only as long as they are required

- Identity-based authorization
  - Limit the privileges granted to an identity

- Attribute-based authorization
  - Use attributes to determine appropriate privileges at this time

- Role-based authorization
  - Assign privileges to roles, and activate roles only when needed

- Capability-based authorization
  - Issue tokens granting only those privileges that are required, for the required lifetime
OAuth and Least Privilege

- OAuth Access Token "scope" identifies specific actions that are authorized on resources in the token "aud" (audience)
- OAuth obtains consent from the resource owner prior to token issuance
- OAuth clients should request only those "scope" values that are required
Developing 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://www.scitokens.org/ for specifications, publications
Visit https://github.com/scitokens for open source implementations
SciTokens
JWT Demo

Visit https://demo.scitokens.org/ and click the "Set Payload" button.

Test the token using the example curl command.
Implementing 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 (reduce "scope")
- draft-ietf-oauth-access-token-jwt: JWT Profile for OAuth 2.0 Access Tokens
  - authorization claims using JWT "scope" and "aud"
Implementing 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
Related Work: GA4GH Passports

- Global Alliance for Genomics & Health (GA4GH)
- Using JWT access tokens with OIDC / OAuth
- Visa types:
  - AffiliationAndRole (e.g., faculty@illinois.edu)
  - AcceptedTermsAndPolicies (e.g., data use terms)
  - ResearcherStatus (e.g., Registered Access Bona Fide Researcher)
  - ControlledAccessGrants (e.g., access to data set #710)
  - LinkedIdentities (e.g., jbasney@xsede.org linked to jbasney@illinois.edu)
- Used in ELIXIR (https://elixir-europe.org/)

https://doi.org/10.1038/s41431-018-0219-y
https://www.ga4gh.org/ga4gh-passports/
Collaboration and Interoperability

● TAGPMA Workshop on Token-Based Authentication and Authorization (Nov 30 - Dec 1 2020)
  ○ https://indico.rnp.br/event/33/
  ○ Participation by WLCG, Globus, LIGO, XSEDE, Fermilab
  ○ Cyberinfrastructure transitioning from X.509 user (proxy) certificates to OAuth/JWT

● Next steps:
  ○ Follow-on workshops
  ○ JWT Profile harmonization
  ○ Hackathons & Interop Testing
Transitioning to Tokens

- With the deprecation of GSI and proxy certificates, we have an opportunity to improve our authorization model
  - We don't want to simply reimplement GSI using JWTs
- Improve security using least privilege capabilities
- Improve usability and interoperability
  - Building on common JWT/OAuth technology
  - Coordinating across projects (LIGO, OSG, WLCG, etc.)
- Maintain the reliability of our infrastructure

- More details in Brian Bockelman's presentation later in this session
Thanks!

Contact: jbasney@ncsa.illinois.edu

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

Join the #scitokens channel in the OSG Slack workspace.

SciTokens Project Team:
Alex Withers, Brian Bockelman, Derek Weitzel, Duncan Brown, Jason Patton, Jeff Gaynor, Jim Basney, Todd Tannenbaum, You Alex Gao, and Zach Miller

This material is based upon work supported by the National Science Foundation under Grant No. 1738962. 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.