The Future of Bearer Tokens

Jim Basney
jbasney@ncsa.illinois.edu

OSG Token Transition Workshop
14 October 2021

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 **bearer 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

Credentials for Authentication / Authorization

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

Authorization / Access Control

		Supported By			
		X.509	SAML	OIDC	OAuth
Identity-based	User identifiers and access control lists	YES	YES	YES	YES
Attribute-based	Access policies based on user attributes	YES	YES	YES	YES
Role-based	Access controls based on group memberships and roles	YES	YES	YES	YES
Capability-based	Tokens allow actions on resources				YES

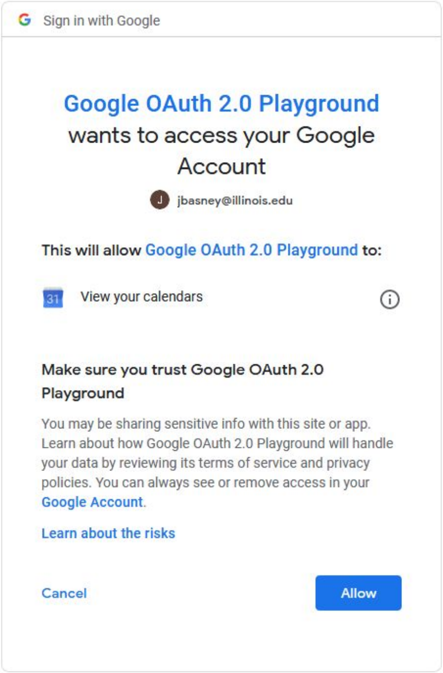
Least Privilege Authorization

- 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 <u>should</u> request only those "scope" values that are required



Sign in with Google

Google OAuth 2.0 Playground wants to access your Google Account

J jbasney@illinois.edu

This will allow Google OAuth 2.0 Playground to:

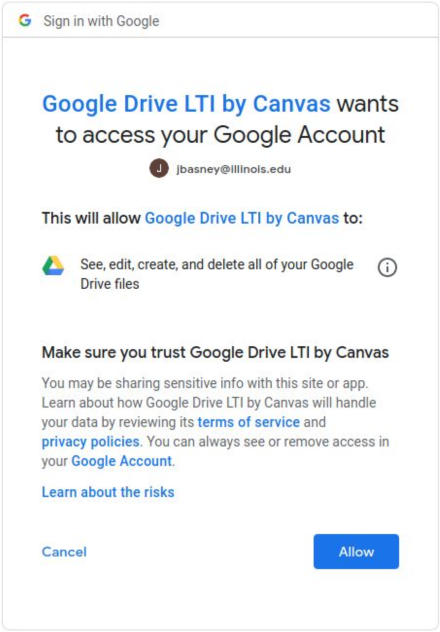
31 View your calendars ⓘ

Make sure you trust Google OAuth 2.0 Playground

You may be sharing sensitive info with this site or app. Learn about how Google OAuth 2.0 Playground will handle your data by reviewing its terms of service and privacy policies. You can always see or remove access in your Google Account.

Learn about the risks

Cancel Allow



Sign in with Google

Google Drive LTI by Canvas wants to access your Google Account

J jbasney@illinois.edu

This will allow Google Drive LTI by Canvas to:

See, edit, create, and delete all of your Google Drive files ⓘ

Make sure you trust Google Drive LTI by Canvas

You may be sharing sensitive info with this site or app. Learn about how Google Drive LTI by Canvas will handle your data by reviewing its terms of service and privacy policies. You can always see or remove access in your Google Account.

Learn about the risks

Cancel Allow

SCI TOKENS

- Capabilities-based authorization 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

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"

RFC
Soon!

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

WLCG

Worldwide LHC Computing Grid

Related Work: GA4GH Passports

Global Alliance
for Genomics & Health
Collaborate. Innovate. Accelerate.

- 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

- Oct 18 2021 Workshop on Token-Based Authentication and Authorization
    - https://sciauth.org/workshop/2021/
    - Participation by CERN, CILogon, Fermilab, INFN, LIGO, OSG, PRP, Tapis, WLCG
    - Cyberinfrastructure transitioning from X.509 user (proxy) certificates to OAuth/JWT
- Ongoing:
    - 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

- Our new **SciAuth** project is focused on helping with this transition

https://sciauth.org/

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!

Contact: jbasney@ncsa.illinois.edu

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

Join the #scitokens channel in the OSG Slack workspace.

SciAuth Project Team:
Brian Bockelman, Derek Weitzel, Jeff Gaynor, Jim Basney

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.

Images provided by Storyblocks (University of Illinois at Urbana-Champaign license).