

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

Jim Basney

jbasney@ncsa.illinois.edu


OSG All Hands Meeting

3 March 2021

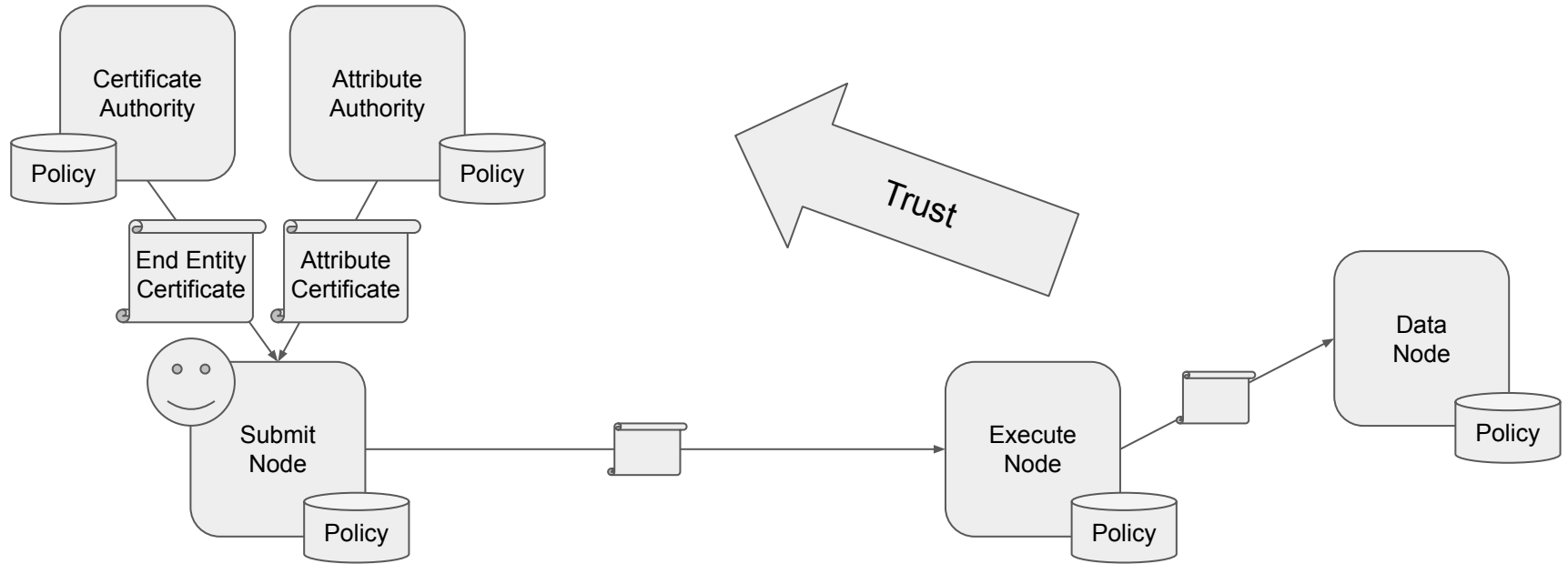
Goals for a dHTC Authorization System

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

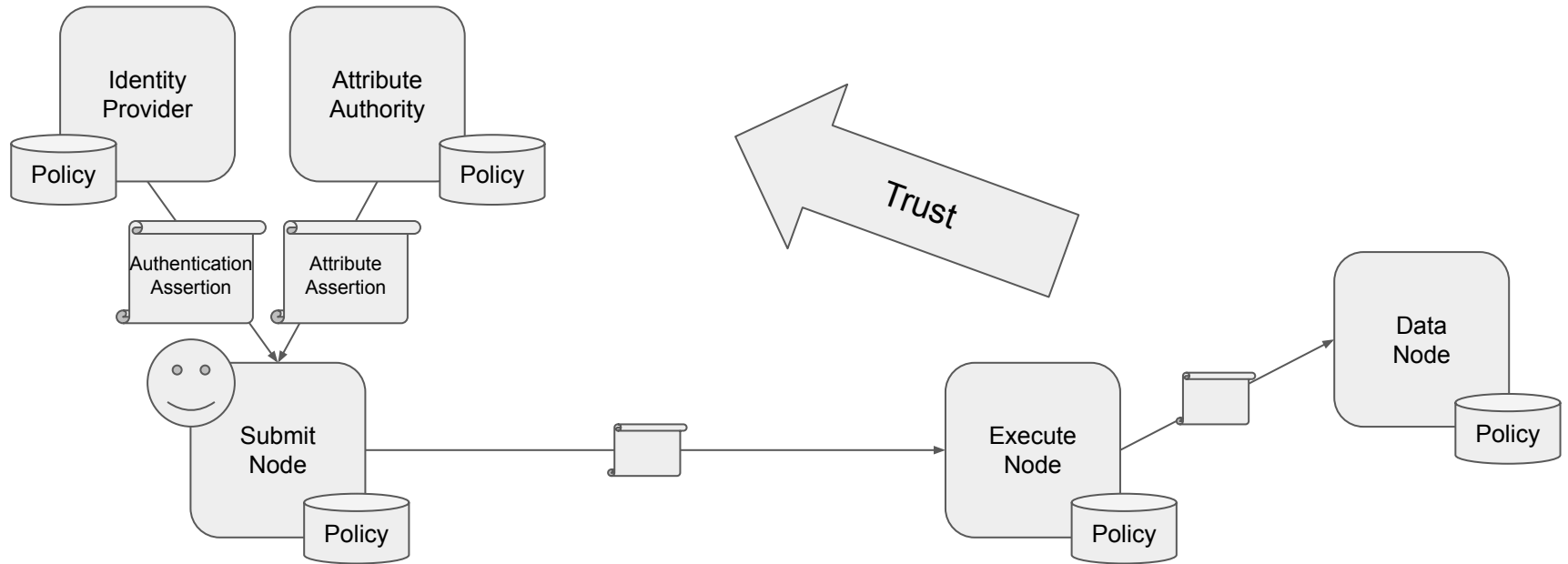
Authentication & Authorization Standards

- 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

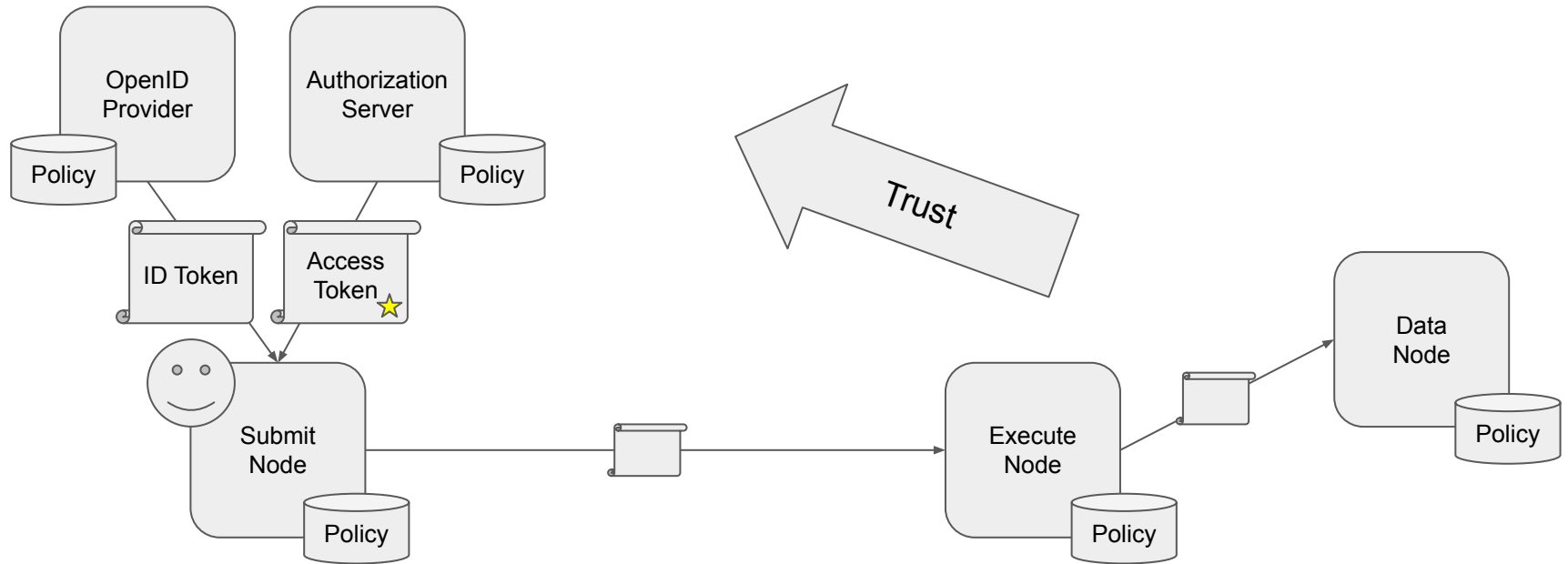
X.509



SAML



JWT / OIDC / OAuth



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 ★

OIDC JWT Demo

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



Success!

- [Show/Hide User Info](#)
- [Show/Hide ID Token](#)

ID Token	eyJ0eXAiOiJKV1QiLCJraWQ0IjIyNDRCMjM1RjZCMjhFMzQxMDhEMTAxRUFENzZmMkM0RSImF5ZyI6IiJUMjU2In0.eyJ1bWVpbCCEmp1YXNuZXI1AaWxse
Header	{ "typ": "JWT", "kid": "244B235F6B28E34108D101EAC7362C4E", "alg": "RS256" }
Payload	{ "email": "jbasney@illinois.edu", "given_name": "James", "family_name": "Basney", "name": "James Basney", "cert_subject_dn": "/DC=org/DC=cilogon/C=US/O=National Center for Supercomputing Applications/CN=James Basney I37233", "idp": "https://idp.ncsa.illinois.edu/idp/shibboleth", "idp_name": "National Center for Supercomputing Applications", "epfn": "jbasney@ncsa.illinois.edu", "eptid": "https://idp.ncsa.illinois.edu/idp/shibboleth!https://cilogon.org/shibboleth!ChF3nEYtvG0S3S1qiwwa5G4Xv0g=", "subject_id": "jbasney@ncsa.illinois.edu", "affiliation": "staff@ncsa.illinois.edu;employee@ncsa.illinois.edu;member@ncsa.illinois.edu", "acr": "https://refeds.org/profile/mfa", "iss": "https://cilogon.org", "sub": "CILL100027", "aud": "cilogon:test.cilogon.org/demo", "token_id": "https://cilogon.org/oauth2/idToken/3cc7a5f035807fe7cf378b0c65ced64/1600985334883", "nonce": "mFuM66sSNZ23NVg79M_qMLrvwYzhPlaqNDZLckC9pXE", "auth_time": "1600985334", "exp": "1600986234", "iat": "1600985334", "isMemberOf": ["CO:members:all", "CO:members:active", "linux-users", "scitokens"] }
Public signing key	-----BEGIN PUBLIC KEY----- MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAhpJRWPFJAv9yolz9ewiLJMkludGZCOJWS XlOwqaTUpWgcvDricRmSOTVxWeDaHig7lprkb7YowOdBv20TWeeNNO1HxTOSnVDwg2jQ8IliR2Gs cwi9pC6gektC9CXEBEEJYn10rx9kazSvMTwXD/92j2t3k8ixbuNzX6ZcfotXe/vmFu7Jtgxr9XYz 2XTM4jXLC4qt02oURVHOMjR0ZsuIIn0wZXvy7kGSonRZgYvyTbpIfevRtVIEye5XPNk-DCBRo76 9qMFCXD1D1Qhc9ePaxLseqht000XEqv8S26MnvjWpuvlXW6GpmVHR6n2tvD2Lk4GU09g3j8rU1Kr sUgfsQIDAQAB -----END PUBLIC KEY-----

- [Show/Hide certificate subject](#)

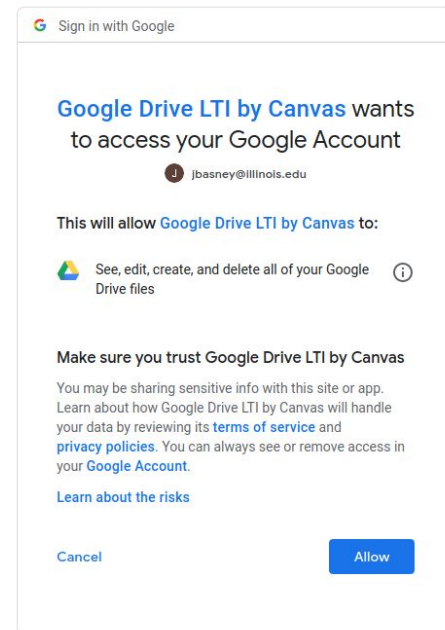
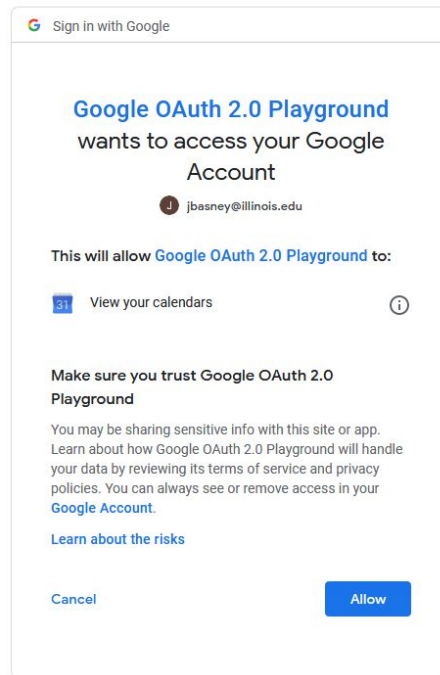
[Return to client](#)

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



SCI TOKENS

- 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.

Token Generator

Use this token generator to create your own sample SciTokens. Typically this would be done as part of an OAuth2 workflow.

Edit the payload of the SciToken on the left. An encoded and signed SciToken will be generated and displayed on the right.

SET PAYLOAD TO ACCESS TO PROTECTED AREA

ALGORITHM RS256

Decoded

EDIT THE PAYLOAD

```
HEADER: ALGORITHM & TOKEN TYPE
{
  "typ": "JWT",
  "alg": "RS256",
  "kid": "key-rs256"
}

PAYLOAD: DATA
{
  "scope": "read://protected",
  "aud": "https://demo.scitokens.org",
  "ver": "scitoken:2.0",
  "iss": "https://demo.scitokens.org",
  "exp": 1614620187,
  "iat": 1614619587,
  "nbf": 1614619587,
  "jti": "616a35df-4b08-461b-ad69-e8af2db83920"
}
```

Encoded

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6ImtleS1yc2I1NiJ9.eyJzY29wZSI6InJlYWQ6L3Byb3RlY3RlZCI6ImF1ZCI6Imh0dHBzOi8vZGVtb5yZ210b2t1bnMub3JnIiwidmVyIjoic2NpdG9rZW46Mi4wIiwiaXNzIjoiaHR0cHM6Ly9kZW1vLnNjaXRva2Vucy5vcmciLCJleHAiOjE2MTQ2MjAxODcsImldCI6MTYxNDYxOTU4NywiImJmIjoxNjE0NTg3LjCjQdGkiOiI2MTZmZkZi00YjA4LTQ2MmwiYXQ2OS10GFmMmRiODM5MjAifQ.0viNWWX6rd0zX_WaQ8r9VU08iVX3ozPjg0sAwcIFD7UK0taFStAP-Ow8w9fh7cx8b_TZZFJtriqvwrPbj6mKzoVaRrgZaSwDowqbWR9X2DT6LZlHlFGG2wLDAT_xBXj6Q3wY7SGbGtb6Tv60SYIsjnskUkMA_WwnSguiZWYnDf-Np02Qc3h2QIrKf1gpMxCHHN7So1IN30DFgwKEo3Gy
```

Signature Verified

Run the curl command below in order to test access to the protected SciTokens area

```
curl -H "Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6ImtleS1yc2I1NiJ9.eyJzY29wZSI6InJlYWQ6L3Byb3RlY3RlZCI6ImF1ZCI6Imh0dHBzOi8vZGVtb5yZ210b2t1bnMub3JnIiwidmVyIjoic2NpdG9rZW46Mi4wIiwiaXNzIjoiaHR0cHM6Ly9kZW1vLnNjaXRva2Vucy5vcmciLCJleHAiOjE2MTQ2MjAxODcsImldCI6MTYxNDYxOTU4NywiImJmIjoxNjE0NTg3LjCjQdGkiOiI2MTZmZkZi00YjA4LTQ2MmwiYXQ2OS10GFmMmRiODM5MjAifQ.0viNWWX6rd0zX_WaQ8r9VU08iVX3ozPjg0sAwcIFD7UK0taFStAP-Ow8w9fh7cx8b_TZZFJtriqvwrPbj6mKzoVaRrgZaSwDowqbWR9X2DT6LZlHlFGG2wLDAT_xBXj6Q3wY7SGbGtb6Tv60SYIsjnskUkMA_WwnSguiZWYnDf-Np02Qc3h2QIrKf1gpMxCHHN7So1IN30DFgwKEo3Gy" https://demo.scitokens.org/protected
```

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!

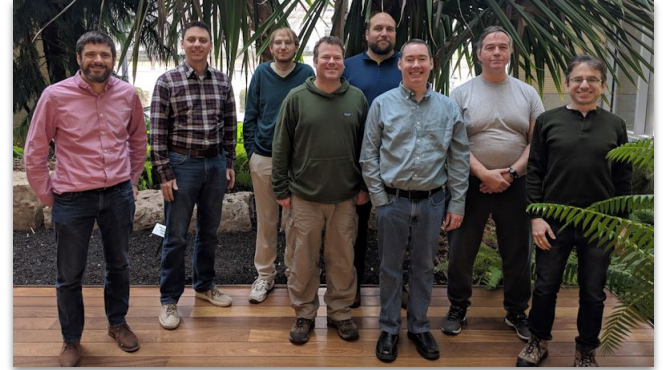
Contact: jbasney@ncsa.illinois.edu

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.