

CILogon

IGTF All Hands Meeting

Jim Basney

jbasney@ncsa.illinois.edu

April 2019

our vision

seamless IAM for academic research collaborations

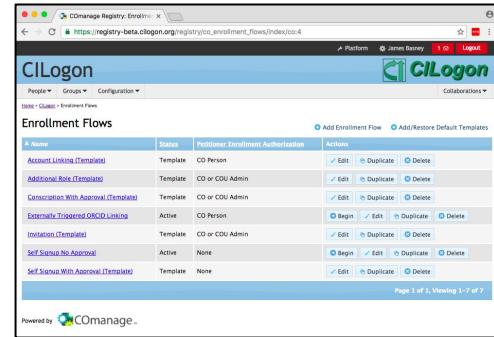
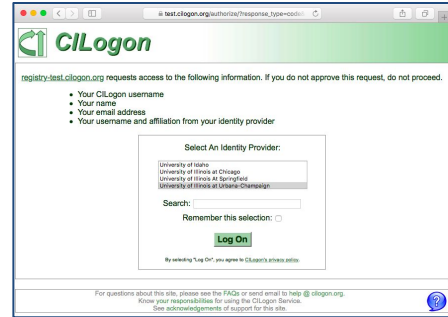
use your campus identity (eduGAIN/Shibboleth)

manage onboarding/offboarding/attributes/groups/roles in one place (COmanage)

integrate with a variety of research apps (OIDC, SAML, LDAP, X.509, SSH)

examples

grid computing
science gateways
jupyter notebooks
campus HPC clusters



Open Source

CILogon (<https://github.com/cilogon>)

OpenID Connect, OAuth, X.509

TIER (<https://www.internet2.edu/tier>)

Shibboleth, COmanage, Grouper

IdentityPython (<https://idpy.org/>)

pyFF, SATOSA

OpenLDAP

our baseline: REFEDS R&S

Attribute release continues to be the #1 stumbling block for new users.



We operate under the REFEDS R&S policy.

Does your campus support REFEDS R&S?

<https://refeds.org/research-and-scholarship>

<https://test.cilogon.org/testidp/>

informed consent

 globus *Powered By*
CILogon 


Globus requests access to the following information. If you do not approve this request, do not proceed.

- Your CILogon username
- Your name
- Your email address
- Your username and affiliation from your identity provider
- A certificate that allows "Globus" to act on your behalf

Selected Identity Provider:

Remember this selection:

By selecting "Log On", you agree to CILogon's privacy policy.

For questions about this site, please see the [FAQs](#) or send email to help@cilogon.org.
Know [your responsibilities](#) for using the CILogon Service.
See [acknowledgements](#) of support for this site. 

our 10 year history

2009 Federated login to TeraGrid.

2010 CILogon operations begin. IGTF X.509 CAs operational.

2011 OAuth support. InCommon Silver support.

2012 Globus identity linking. InCommon R&S.

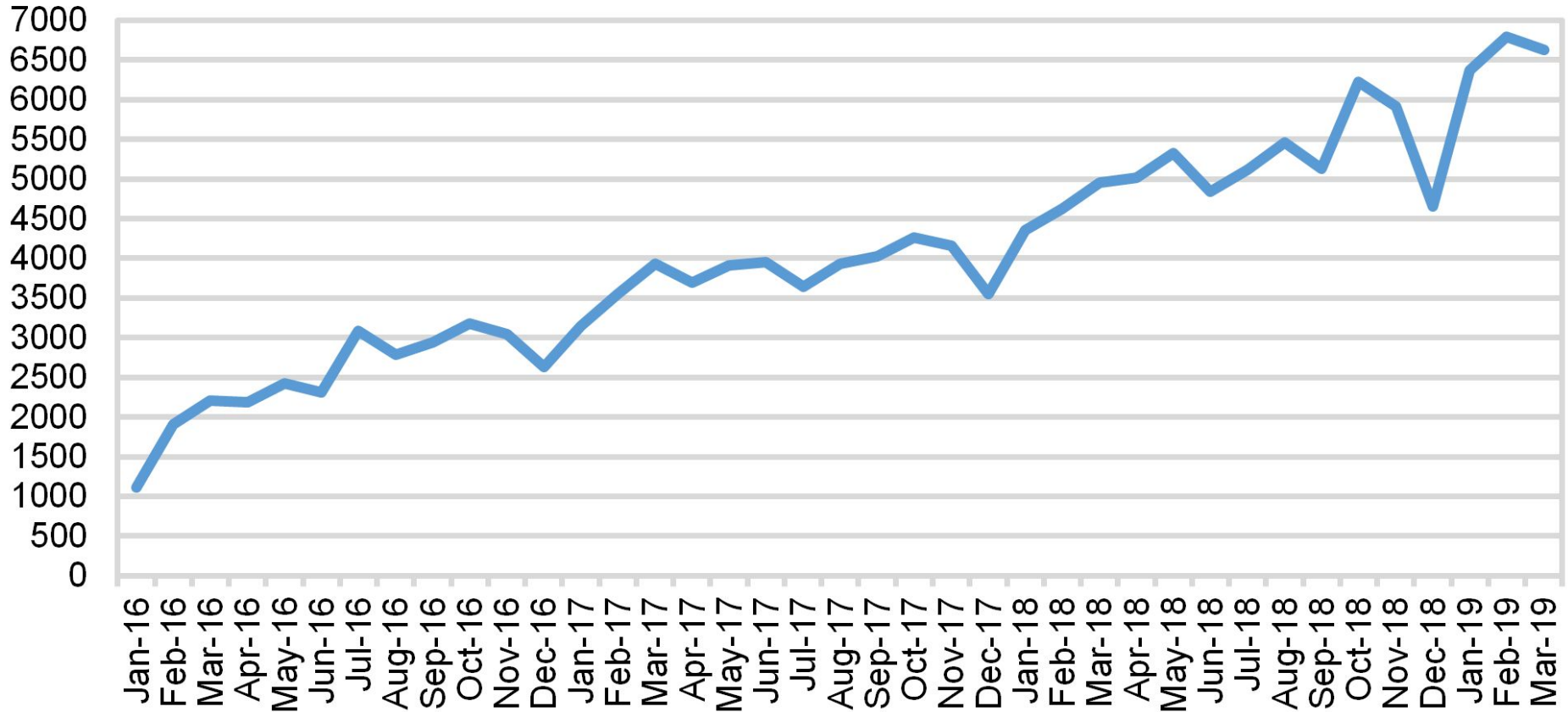
2013 XSEDE operations support. LIGO Data Grid use.

2016 eduGAIN support. OIDC support.

2017 CManage support. AWS deployment.

2019 Transition to subscription funding model.

Active CILogon Users Per Month



our subscription model

Service Tier	Service Rate
Basic Authentication Services	No charge
Basic Multi-tenant Collaboration Management Services	\$1,200 per year
Full Service Production	\$20,000 per year
Custom Support	Contact us

www.cilogon.org/subscribe

CILogon CAs

Certificate Authority	IGTF Profile	certificates issued so far in 2019
OSG CA	classic	4
Basic CA	IOTA	68,411
OpenID CA	experimental	157
Silver CA	MICS	69

CILogon OSG CA Retirement

certificate issuance officially ended May 31 2018

a few certificates manually issued by OSG Security Team
since then

on track to remove CILogon OSG CA from IGTF in July
2019

CILogon OSG CA Retirement

back-end CA operations continue

certificates valid through June 2019

CRL publication and revocation processing
monitoring, incident response, support, etc.

contact: ca@cilogon.org or help@cilogon.org

CILogon Silver CA: History

Originally: A MICS CA based on InCommon Assurance Program

Was Inactive: no InCommon IdPs accredited at Silver level of assurance

Need: Limits to acceptance of IOTA certificates from CILogon Basic CA

CILogon Silver CA: Rebirth

REFEDS Assurance Framework (RAF)

recent pilot with CILogon, XSEDE, others

<https://refeds.org/assurance/IAP/medium> is comparable to
IGTF BIRCH

revised CILogon Silver CP/CPS to use RAF medium/high
(cappuccino/espresso) and now hoping IdPs support it!!!

see <https://ca.cilogon.org/policy/silver>

CILogon Silver CA: Status

operating under new RAF policy since January 2019
certificates issued to BNL and XSEDE users (LIGO next?)

try it out: log on at <https://cilogon.org/>

look for “Level of Assurance: Silver”

if not, log on to <https://test.cilogon.org/testidp/>

Level of Assurance must contain

<https://refeds.org/assurance/profile/cappuccino>

AuthnContextClassRef must contain

<https://refeds.org/profile/sfa> or <https://refeds.org/profile/mfa>



The SciTokens Authorization Model

Illinois: Alex Withers, Jeff Gaynor, Jim Basney

Nebraska: Brian Bockelman, Derek Weitzel

Syracuse: Duncan Brown

Wisconsin: Jason Patton, Todd Tannenbaum, 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.

- The SciTokens project:
 - Introduces a ***capabilities-based* authorization infrastructure** for distributed scientific computing,
 - Provides a **reference platform**, combining CILogon, HTCondor, CVMFS, and XRootD, and
 - **Implements specific use cases** to help our science stakeholders (LIGO and LSST) better achieve their scientific aims.

- 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
- OAuth 2.0 Token Exchange (IETF OAuth WG I-D)
 - token delegation, drop privileges

Example Token, Decoded



- The decoded token contains multiple scopes - basically filesystem authorizations.
- The audience narrows who the token is intended for.
- The issuer identifies who created the token; value used to locate the public keys needed to validate signature.
- The subject is an identifier for the resource owner.
- The expiration is a Unix timestamp when the token expires.

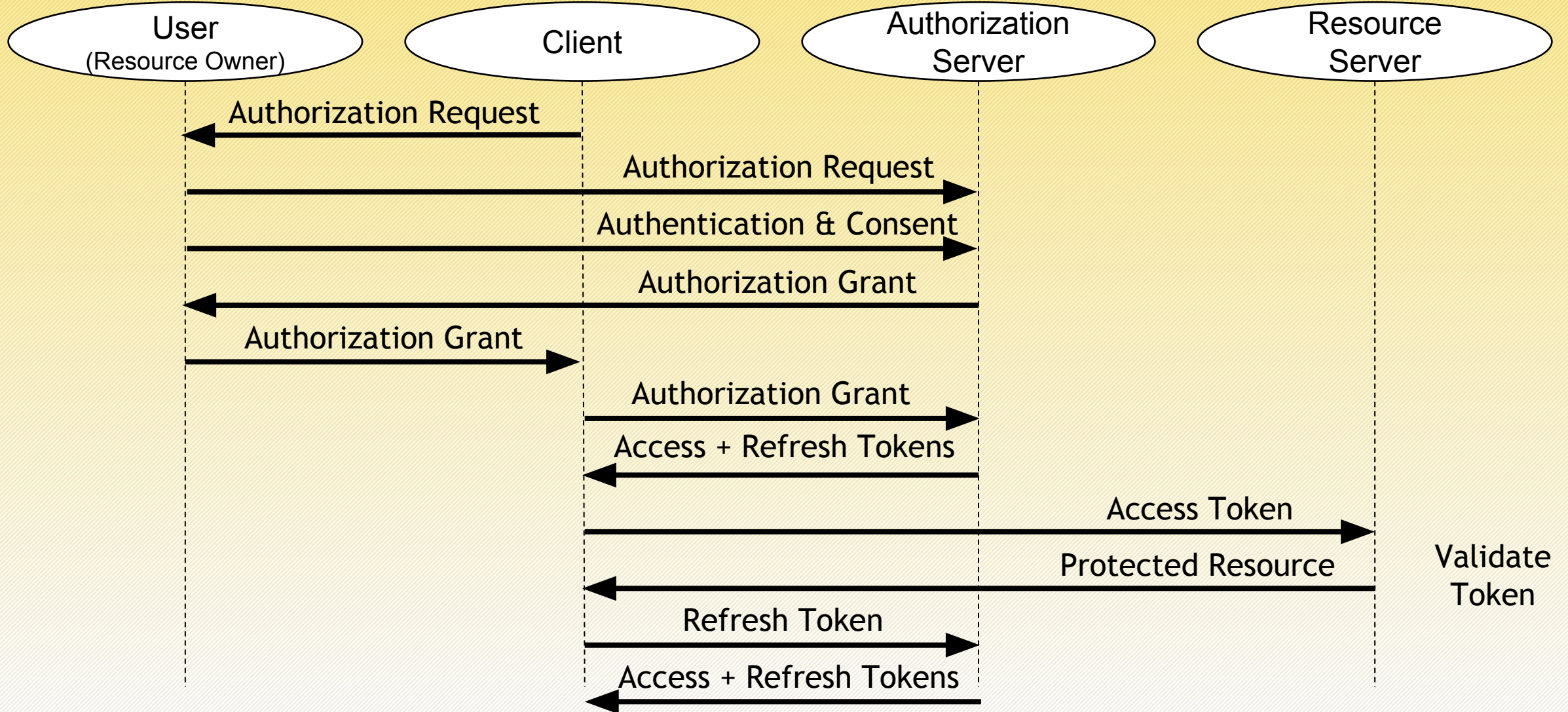
HEADER: ALGORITHM & TOKEN TYPE

```
{  
  "typ": "JWT",  
  "alg": "RS256"  
}
```

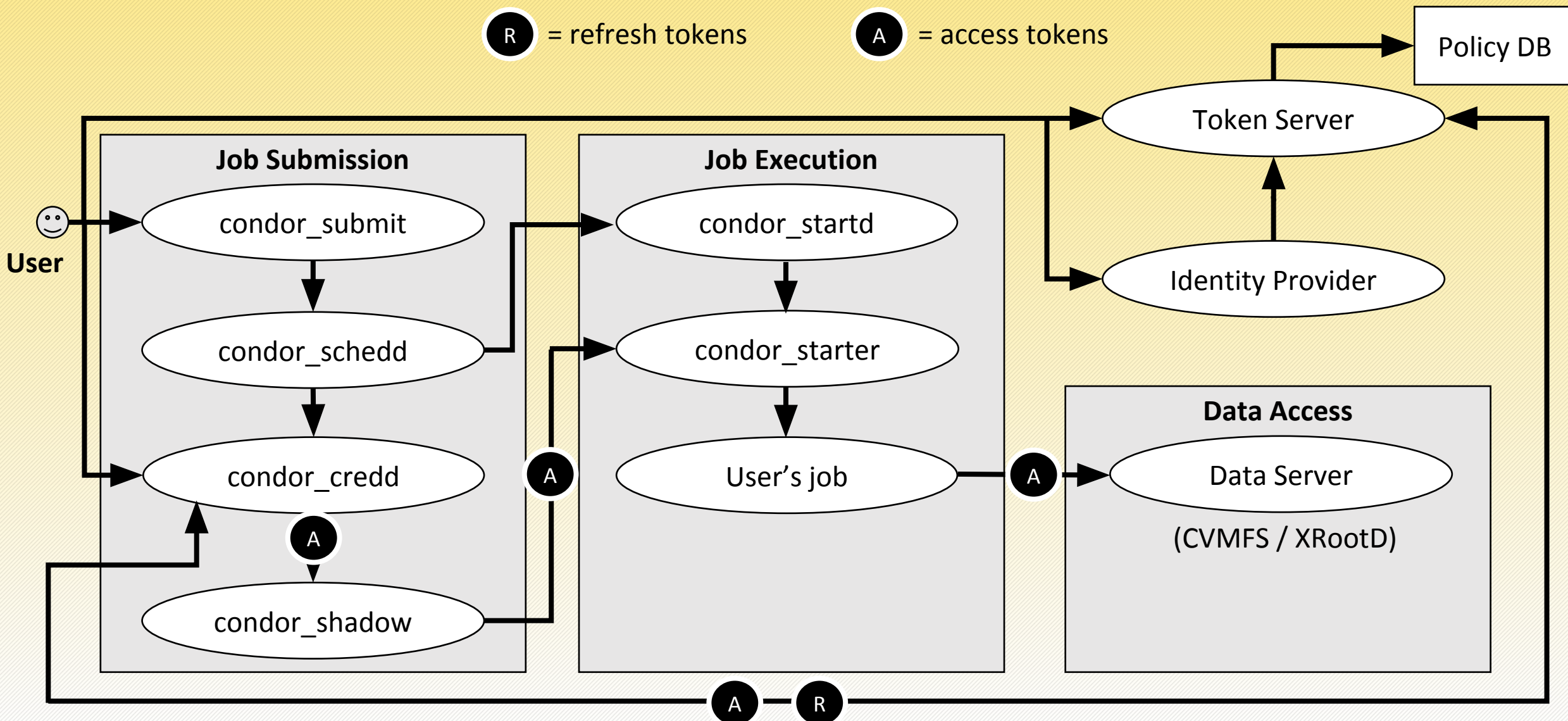
PAYLOAD: DATA

```
{  
  "scope": "read:/protected write:/store/u25321",  
  "aud": "https://demo.scitokens.org",  
  "iss": "https://demo.scitokens.org",  
  "sub": "bbockelm@cern.ch",  
  "exp": 1526954997,  
  "iat": 1526954397,  
  "nbf": 1526954397,  
  "jti": "78c44ce9-62bb-43e8-a7a6-f035f7ebd42b"  
}
```

OAuth2 Authorization Framework



Architecture



CILogon and SciTokens

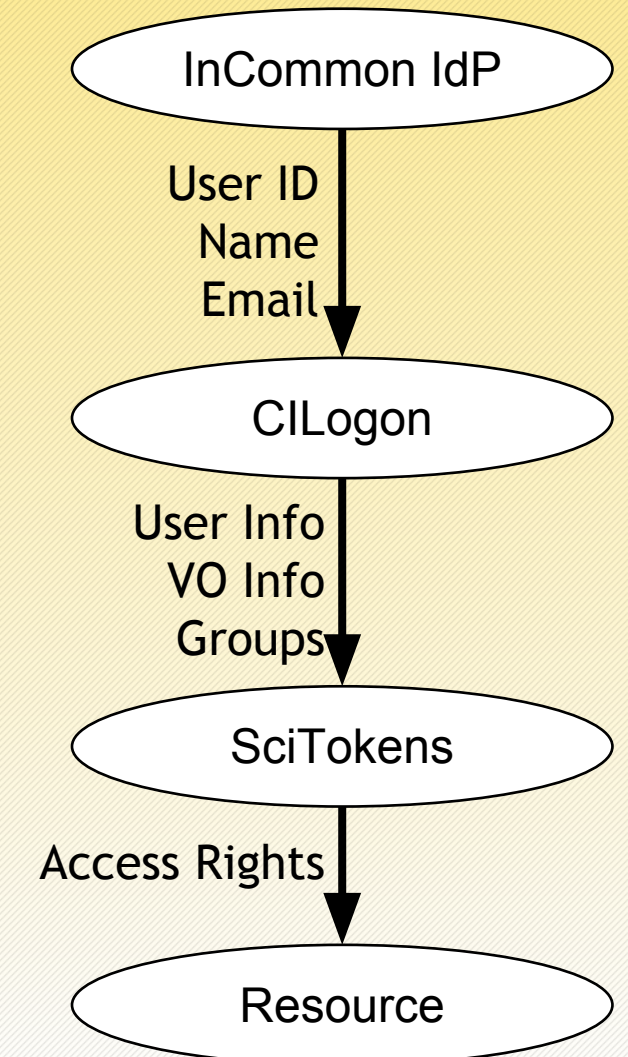
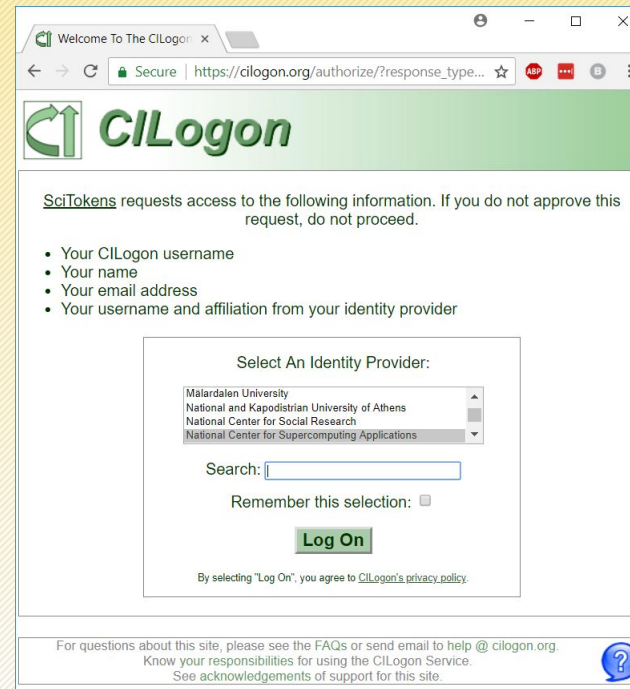


CILogon

- Federated Identity Management
- OpenID Connect
- ID Tokens

SciTokens

- Federated Authorization
- OAuth 2.0
- Access Tokens



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

Grid Community Forum

Community-based support for core software packages in grid computing

<https://gridcf.org/>

Overview

The Grid Community Forum (GridCF) is a global community that provides support for core grid software.

Specifically, the GridCF is attempting to support a software stack christened the Grid Community Toolkit (GCT). The GCT is an open-source fork of the venerable Globus Toolkit created by the Globus Alliance. The GCT is derived from the Globus Toolkit, but is not the Globus Toolkit. Further, the GridCF is not a part of the Globus Alliance.

GCT News

The GridCF is pleased to announce a new release of the GCT: GCT version 6.2.20190226 is a maintenance release and includes all changes since the first GCT 6.2 release in November 2018.

Precompiled packages are available from:

Debian (for Debian unstable (Sid))

EPEL (for Red Hat Enterprise Linux, CentOS and Scientific Linux 6 and 7)

Fedora (for Fedora 28 and 29)

Join the community!

See <https://gridcf.org/> for instructions to join announce@gridcf.org list.

Submit issues and pull requests to: <https://github.com/gridcf/gct>