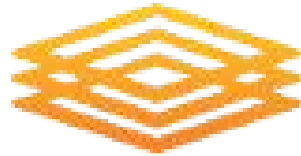


Authentication Modernization at OSG Operations



Authentication & Authorization

Authentication - verifies identity credentials, origin, and validity.



Authorization - determines where you are allowed to go and what you are allowed to do.



Where does OSG use Auth?

OSG Wide Services

- OIM - OSG Information management
 - User/Host certificate management
 - Authorization of privileges
- MyOSG
 - Availability and Reliability metrics
 - Downtime information
 - RSV history and status, etc.
- Ticketing system
- Twiki - OSG Documentation



Focus for
this talk

VO-specific Services

- VO membership management
 - OSG-run VOMS-Admin instances.
 - Don't use VOMS-Admin? *Nothing changes!*

Computing Services:

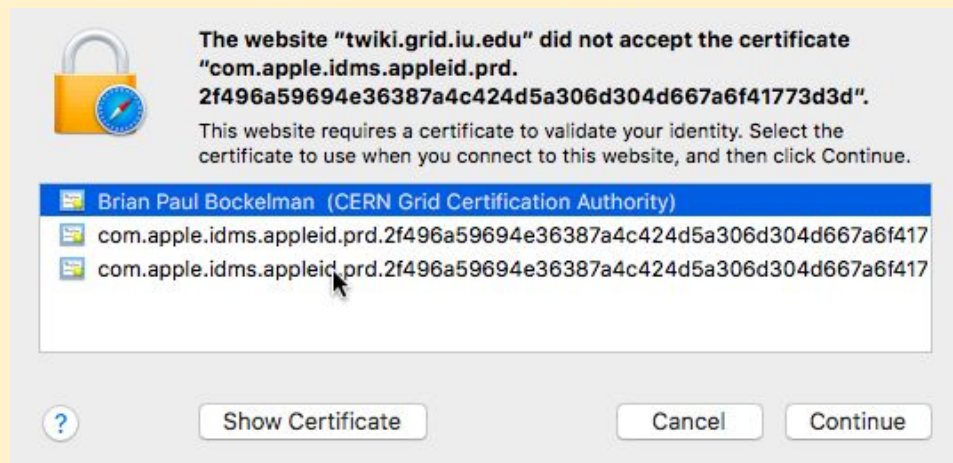
- HTCondor submission services
- HTCondor flocking services
- GlideInWMS factories
- HTCondor Front End

Authentication on OSG

- OSG web services use client X509 certificates for authentication.
 - Users do not know how to manage these in the browser.
 - This is not in line with any other service users utilize.
 - Everyone hates them.

It is harder to edit the twiki than submit jobs on the OSG

Every time a OSG user sees this:



.. curses and puts a penny in a jar

Where we are currently with authentication/authorization

OSG Information Management (OIM)

Pros

- Prevents password sharing, and reuse of the same password
- Does not allow access from an unauthorized computer
- Relies on lightweight OIM (*OSG Information Management System*) authorization matrix
- Auto expires certificate (prevents retention of orphan accounts and unauthorized account access)

Where we are currently with authentication/authorization

Cons

- X509 Certificate installation. Steep Learning Curve.
- Annual Renewal. Long enough to forget. If you forget to renew your certificate you will have to repeat the whole certificate creation process all over again.
- Yet another set authentication credentials.
- Mishandling of the certificates due to the complexity of the usage

What we want to accomplish with a new AAI

- **Authentication:**
 - **Stay out of the authentication business!**
 - Ability to accept federated identity credentials
 - **Trust the identity provider,**
 - Provider handles identity management
- **Authorization:**
 - Current authorization model is OIM database replication for Operational services.
 - To have new robust solution to be interoperable and can be integrated within a wider ecosystem of OSG infrastructure and services
- **The payoff:**
 - **Minimal Learning Curve**
 - Simplified access to Operation services

This modernization is not meant to replace any existing technologies but rather complement existing ones.

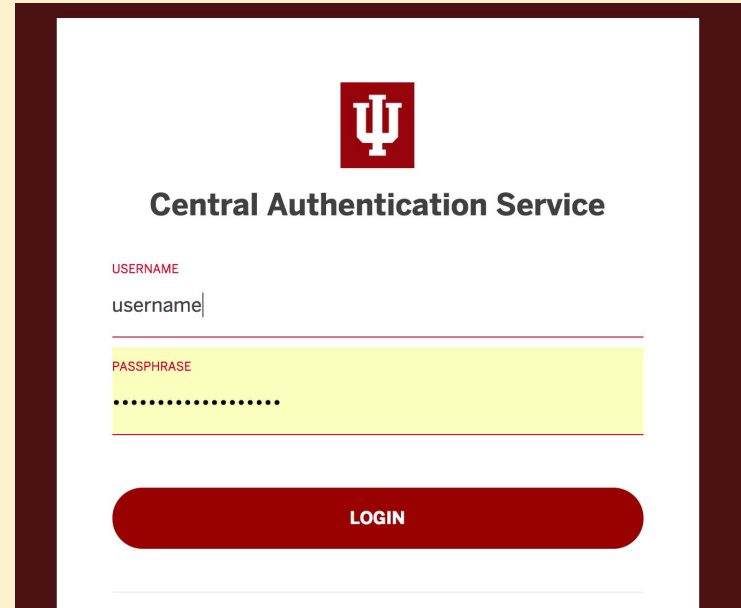
CAS - Central Authentication Service


PROS

- Widely used within academic institutions
- Accepts traditional username/password authentication
- Can be integrated with multiple IdP configurations
- Supports Duo Security
- Easy Integration

CONS

- Limited support & outdated documentation





Central Authentication Service

USERNAME
username|

PASSPHRASE
.....

LOGIN

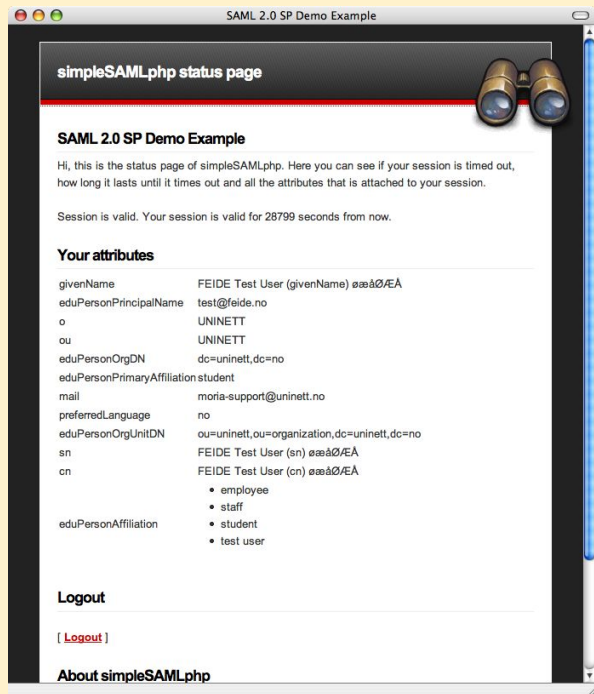
SimpleSAMLphp

PROS

- EGI - AAI Check-In Implementation
- EGI AAI has built-in support for SAML, OpenID Connect and OAuth2 providers
- Open Source, maintained by wide developer community
- Plugin for Comanage Integration & InCommon IdP as well as eduGAIN
- Multiple Commercial Vendors offer support

CONS

- Plugin A la Carte



The screenshot shows a web browser window with the title "SAML 2.0 SP Demo Example". The page content is as follows:

simpleSAMLphp status page

SAML 2.0 SP Demo Example

Hi, this is the status page of simpleSAMLphp. Here you can see if your session is timed out, how long it lasts until it times out and all the attributes that is attached to your session.

Session is valid. Your session is valid for 28799 seconds from now.

Your attributes

givenName	FEIDE Test User (givenName) ø☂/EA
eduPersonPrincipalName	test@feide.no
o	UNINETT
ou	UNINETT
eduPersonOrgDN	dc=uninett,dc=no
eduPersonPrimaryAffiliation	student
mail	moria-support@uninett.no
preferredLanguage	no
eduPersonOrgUnitDN	ou=uninett,ou=organization,dc=uninett,dc=no
sn	FEIDE Test User (sn) ø☂/EA
cn	FEIDE Test User (cn) ø☂/EA <ul style="list-style-type: none">• employee• staff• student• test user
eduPersonAffiliation	

Logout

[[Logout](#)]

About simpleSAMLphp

CILogon 1.0

PROS:

- Provides easy integration with InCommon federation.
 - Works with Open ID Connect, one of the most popular authentication protocols.
 - Every OSG user has an InCommon identity.
 - Higher Education Participants (619)
 - Government and Nonprofit Laboratories, Research Centers, and Agencies (30)
 - Sponsored Partners (268)

CONS:

- Does not provide authorization.
- Cannot touch VO membership use case.

CILogon

[Show Help](#)

Select An Identity Provider:

- Imperial College London
- IMT Institute for Advanced Studies Lucca
- INALCO - Institut National des Langues et Civilisations O
- Indiana University

Search:

Remember this selection:

Log On

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.

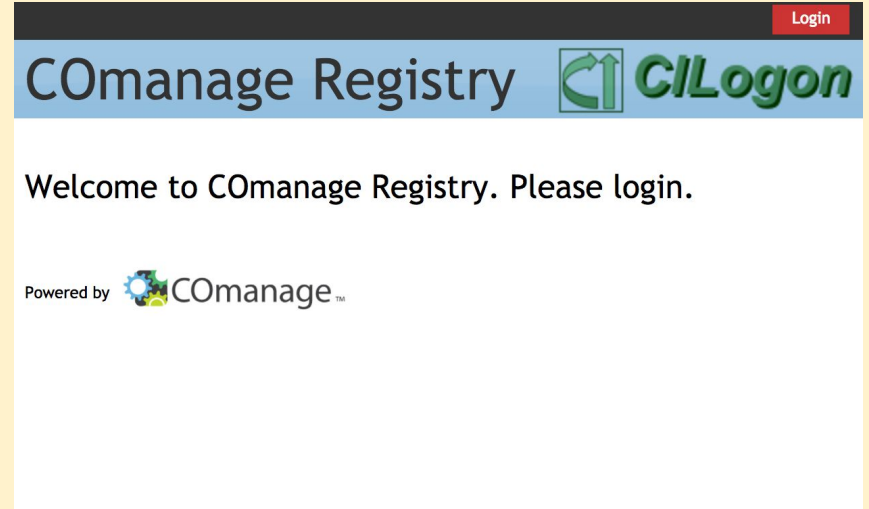
CILogon 2.0

PROS

- CILogon 1.0 + Comanage
- Integrated with InCommon Federation
- Comanage features
 - SSH key management
 - Multi Factor Authentication
 - Groups, roles, & privileges
- Hosted solution by CILogon
- Supported by CILogon
 - Makes implementation, supports & maintenance simple and straightforward

CONS

- BETA stage
 - 3 year project. Currently at year 1.



Next steps

Communicate / Collaborate with OSG stakeholders

Make sure our planned scope and direction of software, technologies and partners fits well with our community.

Selection of the SSO technology

Robust solution to be able to accommodate OSG-run web properties.

Demo applications

....