InCommon Federation Experiences

Jim Basney
jbasney@ncsa.uiuc.edu

This material is based upon work supported by the National Science Foundation under grant number 0943633. 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.
Service Provider Perspective

go.teragrid.org
- Campus logon to TeraGrid
- 34 IdPs supported so far
- Attributes:
  - Persistent user identifier

cilogon.org
- Campus or OpenID logon to CI
- 40 IdPs supported so far (3 OpenID)
- Attributes:
  - Persistent user identifier
  - Given name and Surname
  - Email address
Key SP Decisions

• Choose your EntityID(s)
  – Unique URI that identifies your SP
  – Need not match your service locations
  – Carefully decide when to use different EntityIDs
  – https://spaces.internet2.edu/x/eAUjAQ

• Determine what attributes you need
  – http://www.incommon.org/attributes.html

• Very difficult to change later!
  – IdP attribute release policies based on EntityID
  – Example: TeraGrid’s name is changing this year, but we’re keeping our teragrid.org EntityID
SP Registration Example

InCommon Site Admin: Teragrid of the University of Chicago

Your Service Provider

Provider ID:
https://go.teragrid.org/shibboleth

User Interface Elements and Requested Attributes:

User Interface Elements:
- Display Name: Teragrid
- Description: The Teragrid project, funded by the National Science Foundation
- Information URL: https://go.teragrid.org/
- Privacy Statement URL: https://www.teragrid.org/web/user-support/allocation_policy
- Logo URL: https://go.teragrid.org/logo
- Logo Width and Height: 809 x 275 (pixels)

Requested Attributes:
- eduPersonTargetedID

Key Name: go.teragrid.org (Serial #13632501242686897071) Use: Signing and Encryption

Contact Type: Support
Contact Name: Teragrid InCommon Support
Contact Email: go-admin@teragrid.org

Contact Type: Technical
Contact Name: Teragrid InCommon Support
Contact Email: go-admin@teragrid.org

Contact Type: Administrative
Contact Name: Teragrid InCommon Support
Contact Email: go-admin@teragrid.org
SP Registration Example
User Attribute Options

• Attributes from campus
  – If IdP is willing to release
  – What level of assurance?

• Prompt user to enter self-asserted attributes
  – Most flexibility
  – Inconvenient for users

• SP-specific attribute establishment process
  – Example: TeraGrid allocations process
  – Example: Virtual Organization membership

• cilogon.org needs more attributes from campus than go.teragrid.org, which uses TeraGrid user DB
Persistent User Identifier

- **eduPersonPrincipalName (ePPN)**
  - Example: jbasney@illinois.edu
  - NOT guaranteed to be a valid email address
  - MAY be reassigned (after some hiatus period)

- **eduPersonTargetedID (ePTID)**
  - Example:
    urn:mace:incommon:uiuc.edu!https://cilogon.org/shibboleth!
    cyXC3O5fi0t1NBsW1NsOxZDyDd4=
  - MUST NOT be reassigned
  - REQUIRED to be opaque
  - Designed to preserve the principal’s privacy and inhibit the ability of multiple unrelated services from correlating principal activity by comparing values
ePPN vs ePTID

• Concern about reassignment
  – If IdP sends ePPN, TeraGrid needs to know reassignment policy
    • Forces an IdP vetting process
  – TeraGrid requires annual account linking, motivated in part by reassignment concerns

• Of 34 go.teragrid.org IdPs:
  – 16 release ePTID
  – 16 release ePPN and never reassign
  – 2 release ePPN and reassign with >1yr hiatus
Account Linking

Welcome University of Illinois at Urbana-Champaign User

Associate Identity With TeraGrid Username

It appears that this is the first time you have logged on to this site with your Identity provided by University of Illinois at Urbana-Champaign. In order to utilize TeraGrid resources, you must first log in to your TeraGrid account. You will use the same username and password you use to log on to the TeraGrid User Portal.

This step needs to be performed only once for each identity. Future logins with your Identity will be associated with your TeraGrid username, thus bypassing this step.

Note that this step only verifies that you can log in to TeraGrid with a particular username. No password information is stored on this site.

Log in to TeraGrid

Username: jbasney
Password: ***************

Forgot your password?

Manage Associations

Below is a table showing all identities associated with TeraGrid username "jbasney". If you want to delete any of them, check the appropriate box in the "Delete?" column and click the "Delete Checked" button.

If you delete the association for the current Identity (shown in italics), you will be required to log in to TeraGrid again to re-establish the association.

Delete? | Identity Provider | Created | Last Access
--------|-------------------|---------|------------
[ ] | University of Illinois at Urbana-Champaign | 2010-06-06 13:05:28:28 | 2010-04-06 13:09:47:05

Delete Checked

Go Back

The TeraGrid project is funded by the National Science Foundation and includes eleven resource providers: INDIAN, LONI, NCA, NCSA, NCE, ORNL, PSC, Purdue, SDSC, TACC and UCB.

Please send any questions or comments about this site to go-admin@teragrid.org.

The project uses software from the MyProxy and GridShib projects.

Please send any questions or comments about this site to go-admin@teragrid.org.
User Names

CiLogon uses:

• **givenName** and **sn** (surname)
  – Multi-valued attributes

• **displayName**
  – “preferred name of a person to be used when displaying entries”

• **cn** (common name)
  – “impossible to give a precise and accurate definition of what this field means”

• **eduPersonNickname**
  – “the person's preferred nickname(s)”

All IdPs provide to CiLogon (so far)
SP On-Boarding

• Goal: Enable successful use of SPs by users from many IdPs
  – Particularly difficult for “no contract” SPs (“user-driven” SPs)
• Challenge: Attribute release
  – Technical solutions: user consent, attribute requirements in metadata, IdP filtering
  – Policy: privacy, FERPA, SP trust
    • Policies differ for students versus faculty/staff
    • Scaling: attribute bundles, default release policies
SP On-Boarding

Login Unsuccessful

Your Identity Provider did not release enough information for our services to properly identify you. You will need to contact an Identity Provider administrator to enable the release of the appropriate information, or alternatively use an alternative Identity Provider with a more liberal policy.

You may direct your technical staff to this infrastructure page for specific technical details on configuration and our policies regarding the information we receive.
CILogon Service

Test Your Organization's Identity Provider

Verify SAML Attribute Release Policy
Thank you for your interest in the CILogon Service. This page allows the administrator of an Identity Provider (IdP) to verify that all necessary SAML attributes have been released to the CILogon Service Provider (SP). Below you will see the various attributes required by the CILogon Service and their values as released by your IdP. If all required attributes are present, you can add your IdP to the list of organizations available to the CILogon Service (assuming it has not already been added).

Summary
- All required attributes have been released by your IdP. For details of the various attributes utilized by the CILogon Service and their current values, see the sections below.

Add Your IdP to the CILogon Service

SAML Attributes
- Identity Provider (entityID): urn:mace:incommon:uiuc.edu
- ePTID:
- ePPN: jbasney@illinois.edu
- First Name (givenName): James
- Last Name (sn): Basney
- Display Name (displayName): James Alan Basney
- Email Address (email): jbasney@illinois.edu
- Level of Assurance (assurance):

Metadata Attributes
- Organization Name: University of Illinois at Urbana-Champaign
- Technical Contact: Mike Grady <m-grady@uiuc.edu>
- Administrative Contact: Mike Grady <m-grady@uiuc.edu>
“Homeless” Users

• Handling users w/o institutional logins
  – Home institution not (yet) in InCommon
  – Home institution not (yet) on-boarded w/ SP

• go.teragrid.org
  – TeraGrid username/password
  – ProtectNetwork

• cilogon.org
  – “Request a New Organization” page
  – OpenID (Google, PayPal, VeriSign)
  – ProtectNetwork
  – Coming Soon: project logins (LIGO, LTER, …)
Multiple Federations: Example

- go.teragrid.org supported both InCommon and University of Texas System
  - Easy to configure Shibboleth to load multiple metadata sources
  - Our custom discovery service showed IdPs from both federations
  - No longer needed now that UT System has joined InCommon
Levels of Assurance

- LOA requirements differ across scientific collaborations
  - 2-factor authentication
  - International Grid Trust Federation
  - Open access with usage statistics
- CILogon LOA options:
  - InCommon Silver: US Gov’t ICAM Level 2
  - OpenID OIX: US Gov’t ICAM Level 1
  - InCommon “Basic”
Non-Browser Use Cases

• Currently CILogon requires browser-based authentication (SAML, OpenID)
  – With certificate retrieval & use supported outside the browser

• CILogon support for SAML Enhanced Client or Proxy (ECP) coming soon
  – For end-to-end command-line certificate issuance
  – ECP adoption by InCommon campuses beginning

• Also watching Project Moonshot
  – US eduroam (RADIUS) adoption growing
A Roadmap for Using NSF Cyberinfrastructure with InCommon

A helpful guide for CI projects

http://www.incommon.org/cyberroadmap.html
Thanks

For more information:

www.cilogon.org

info@cilogon.org