**Federated Login to TeraGrid**

Jim Baaney  
Terry Fleury  
Von Welch

This material is based upon work supported by the National Science Foundation under Grant No. 0503697

---

**Goal**

- Enable researchers to use the authentication method of their home organization for access to TeraGrid
- Researchers don’t need to use TeraGrid-specific credentials
- Avoid distribution of TeraGrid-specific passwords
- Avoid TeraGrid password reset requests
- Better integrate TeraGrid with campus resources
- Provision TeraGrid resources according to campus-based identity vetting and authorization

---

**Challenges**

- Support TeraGrid usage models
  - Interactive browser and command-line access
  - Multi-stage, unattended batch workflows
- Establish trust among campuses, TeraGrid members, and peer grids (OSG, EGEE)
**TeraGrid Allocations**

- Resources allocated by peer review
- Project principal investigators add user accounts via the User Portal
- Central Database (TGCDB) contains records for all users
- TeraGrid-wide username and password assigned to every user

**Federated Login to TeraGrid**

**InCommon Federation**

- InCommon facilitates use of campus identity with external service providers
  - By supporting adoption of standard mechanisms and policies
  - By distributing metadata that identifies members
- Uses SAML Web Browser Single Sign-On protocols
  - Shibboleth implementation from Internet2
  - Work well for browser-based applications, but not command-line or batch workflows
- InCommon represents >200 institutions (>4m users)
  - Of 38 institutions with over 50 TG users, 24 (67%) are currently InCommon members

**TeraGrid Single Sign-On**

**TeraGrid PKI**

- TeraGrid PKI consists of CAs operated by TeraGrid member institutions and other partners
- TeraGrid resource providers trust a consistent set of CAs
  - Provides consistent experience for users
  - Determined by consensus through Security Working Group
  - CAs accredited by International Grid Trust Federation (IGTF)
Our Approach

• Account Linking
  - Bind the researcher’s campus identity (conveyed via InCommon/SAML) to his/her existing TeraGrid identity (TGCDB)
  - InCommon motivates our use of SAML
  - Rely on the existing TeraGrid allocations process for identity vetting and authorization
  - Rely on campus for authentication of a persistent user identifier

• Credential Translation
  - Convert from a browser-based (SAML) credential to a certificate for command-line, workflow, and batch processes
  - Deliver certificate to desktop and web session
  - Rely on the existing TeraGrid PKI
  - Adding a new certificate authority

User Experience
**Federated Login to TeraGrid**

### Trust Establishment

- Campus and InCommon
- TeraGrid PKI

### Trust Establishment Process: Campus

- Join the InCommon Federation
- Add service provider to InCommon metadata
- Request identity providers to release identity information (a manual, campus-by-campus process)
  - Some released identifiers automatically to all InCommon members
  - Some released identifiers on email request
  - Some required local sponsorship and review
- Current status:
  - Targeted 38 campuses with over 50 TeraGrid users
  - 24 (67%) are InCommon members
  - 16 (of the 24) successfully federated to-date
  - 11 additional campuses federated outside the target list
Trust Establishment Process: PKI

- Publish Certificate Policy and Certification Practices Statement (CP/CPS) according to RFC 3647
- Present CA to regional IGTF policy management authority – The Americas Grid PMA (TAGPMA)
- Checklist-based review by TAGPMA of CA’s policies and operations
- Vote for acceptance by TAGPMA members
- Current status:
  - Submitted to TAGPMA (March 2009)
  - Approved by TAGPMA (May 2009)
- CA certificate included in TERENA Academic CA Repository (TACAR)

Security Considerations

- Changes to TeraGrid trust architecture
  - Adding InCommon identity providers as trusted entities
  - Adding web authentication as a trusted method
- Peering with identity providers (IdPs)
  - IdP decides whether to release identifiers to TeraGrid
  - TeraGrid decides to accept IdP assertions – review includes:
    - IdP serves TeraGrid users
    - IdP is operated by a known and respected organization
    - IdP operates a trustworthy authentication service
    - IdP provides globally-unique and non-reassigned identifiers

Security Considerations

- Web application security
  - Use HTTPS for privacy and authentication
  - Cross-Site Request Forgery (CSRF) attack protections (cookies and hidden form fields)
  - Locked down servers (firewalls, OTP for admin access, etc.)
- CA security
  - FIPS 140 level 2 rated hardware security modules
  - Locked down servers
Security Considerations

- Disallowing account sharing
  - Account sharing complicates incident response
  - Allow only one identifier per identity provider to be linked with a given TeraGrid identity

- Incident response
  - Actions may include:
    - Disable account links
    - Disable identity provider trust
    - Revoke certificates
    - Coordinate response with TeraGrid security working group, InCommon, and IGTF

Related Work

- Federated CAs (some accredited by IGTF) in Europe:
  - Switzerland: SWITCH SLCS CA for SWITCHaai federation
  - Germany: DFN-SLCS CA for DFN-AAI federation
  - UK: SARoNGS Credential Translation Service for UK Access Management federation
  - TERENA Certificate Service for national federations (Denmark, Finland, Netherlands, Norway, Sweden, and more)
- TeraGrid Science Gateways
  - Web-based community access to TeraGrid resources
  - Gateways manage their own user registration and authentication
  - May independently support federated login

Status

- In production at https://go.teragrid.org since Sep 2009
  - Supporting logins from 27 institutions
  - Issued >800 certificates so far
- Work in progress:
  - Integrate with TeraGrid User Portal (https://portal.teragrid.org)
  - CILogon Project (www.cilogon.org)
    - Provide certificates to all InCommon members (not just TeraGrid users)
  - Other possible future work for TeraGrid:
    - Phase out TeraGrid passwords
    - Attribute-based authorization
    - Support for OpenID

Questions? Comments?

- Contact: jbasney@illinois.edu