Case Studies in Identity Management for Virtual Organizations

February 22, 2007

Paul Caskey  UT-System
Margaret Murray, Texas
Advanced Computing Center
Jerry Perez, Texas Tech U.
Alan Sill, Texas Tech U.
• **Overview and Session Goals** (Sill)

• **The U.T. System IdM Federation** (Caskey)
  - History, Status, Lessons Learned and Future Plans
  - A Member-Integrated X.509 PKI service

• **SURAgrid Two-tier PKI** (Perez)
  - Bridge CA and LDAP use
  - Integration and Comparison with other PKI services

• **Identity Management in Grids** (Sill)
  - The IGTF, VO servers, standards and technology trends
  - TIGRE integration with multiple grids
Overview and Goals

• This session will focus on **practical examples** for identity management between members of academic institutions involved in virtual organizations of several types.
• The idea of a **Virtual Organizations** in academic settings will be defined and explored.
• Specific examples involving **actual use cases** with **functioning organizations** will be given.
• These examples are meant to be **illustrative**, not to unduly define or restrict the space of discussion.
A Virtual Organization (VO) is any collective group that operates in a coordinated way to enable shared activities on one or more topics with common tools or governance.

VOs can exist within institutional boundaries but are most effective when constituted to operate across and to unify participants in different physical or institutional limits.

Primary purpose is to pursue the shared topic or topics.
Examples of Virtual Organizations

- LHC Computing Grid experiments (CMS, Atlas, Alice)
- Cancer Biomedical Informatics Grid
- SCOOP (SURA Coastal Ocean Observing Project)
- Participants in the Open Science Grid
- Texas Internet Grid for Research and Education
- Individual universities
- University systems
- Industry organizations
- Individual researchers and research groups
- Collections of the above
Virtual organizations are increasingly becoming the *primary paradigm* to enable work to take place in discipline-specific ways across institutional physical boundaries for essentially all fields.

Another word for this is “Academics.”

This is the *core function* of our individual academic institutions and research efforts.

It is NOT optional, and to enable it to go forward we need good I.T. tools.
• The Burton group defines IdM as: “A set of processes, and a supporting infrastructure, for the creation, maintenance, and use of digital identities.”
• It is more than account creation, more than directories, authentication, access controls, etc.
• More than just technology, IdM includes policy, process, governance, trust, and new ways of thinking about I.T.
IdM is important because it requires and enables provision of and compliance with needs of:

• Regulation
  ▪ HIPAA, FERPA, SOX, GLB, etc.
  ▪ Audit trails and tracking

• Security
  ▪ Application Security / LoA-based access

• Collaboration
  ▪ Virtual Organizations
  ▪ Shared Services
IT TAKES A FEDERATION:

Creating and Extending UT System IdM

Paul Caskey  UT System
Margaret Murray, Texas Advanced Computing Center
• What is IdM Federation?
• SWITCH, the Swiss Higher-Ed Federation defines it as "A collection of organizations that agree to interoperate under a certain ruleset."
• A simple definition, but, in practice, loaded with complexity.
• Example: Shibboleth, an Internet2 implementation of the SAML protocol, is a software package that enables federations.
• Shibboleth itself does not enable VOs, but can be configured to work with them.
• IdM Federation within the UT System started with the IdM Statement of Direction created and published by the U.T. System Strategic Leadership Council

• Funding from an NMI-EDIT ETR grant

• “Shib-Fest” used to launch the process

• Transition to Production Operations
U.T. System IdM Components

Policy
• Charter, Fees, Attributes, FOP, MOP
• LoA

Technology
• 17 IdPs
• 10 federated apps
• 1 external vendor

Governance
• IdM Governing Board: Technical Operations, Policy Mgmt
• Audit
• Dispute resolution
**How Does Shibboleth Work?**

1. **Who are You? Can you login?**
2. **What is your Organization?**
3. **What are the attributes for this user?**
4. **I know who you are. Your request and handle is redirected to SP.**
5. **The allowed attributes are returned to the SP.**
6. **I am satisfied with the attributes. Control is passed to the application.**

---

**Identity Provider**

- Handle Service/SSO
- Attribute Requestor
- Resource Manager/Svr Module
- LDAP (eduPerson)

**Service Provider**

- User/Web browser
- WAYF (Federation)
- Assertion Consumer Service
- Attribute Provider
- Web application
- Web Site

---

**Flow:**

1. Your request is forwarded to your Organization’s IdP HS/SSO
2. I need more information.
3. Now I know you are someone. I need more information.
4. What are you asking for and does it require a shibb session?
5. What is your Organization?
6. Home campus
7. Web application
8. What are the attributes for this user?
9. LDAP (eduPerson)
10. Attribute Provider
11. The allowed attributes are returned to the SP.
Source:

Color Key:
- Complete
- Current Development
- In-Progress
- Longer-term Future
• Policy work is critical and slow - start early!
• Don't underestimate the difficulty of application integration with new or legacy infrastructure – go for the low-hanging fruit first.
• Selling infrastructure is hard.
• Consider new support models.
• Communication and coordination are key.
• Shared services on a grand scale may offer benefits for:
  ▪ Licensing
  ▪ Support
  ▪ Administration
• Inter-federation trust fabric (TDL, TIGRE, HAM-TMC)
• Shared Learning Management System (LMS) and HR/Benefits applications
• Access to grid computing resources
• Facilitate access to myriad applications
  ▪ Easy to plug right in to the infrastructure
• Note: Shibboleth *by itself* does not enable VOs to operate, but work is going on in many sectors to enable federated identity to be used with grids.

• UT System pursuing work with TACC to enable system IdM to be used to provide strong credentials to be used by grid researchers.

• International Grid Trust Federation (IGTF) is the accrediting body for grid authentication CAs.

• TACC is accredited with the IGTF and is developing a new Member Integrated Credential Service (MICS).
• Primarily used for “low LoA” applications

• Required: *(for ANY username/password pair)*:
  - Enforce use of encrypted SSL/TLS channel
  - Enforce password length, validity duration and complexity requirements

• Optional *(but becoming increasingly important)*:
  - Enforce Level of Assurance 2 (in-person vetting)
  - Use with an external identity token
  - Combine with X.509 certificate signed by an accredited Certificate Authority (CA)
  - Separate portal login from HPC resource login
  - Use pool or gateway accounts
• Public Key Infrastructure (PKI):
  ▪ Users generate separate public/private key pairs
  ▪ Users exchange their public keys
  ▪ User A encrypts message with User B's public key
  ▪ Only User B can decrypt User A's message using User B's private key
• Certificate Authority acts as a root of trust
  ▪ Issues and manages X.509 credentials
  ▪ Based on registration authority (RA) vetting of user
  ▪ Allows credential checking
  ▪ Establishes certificate expiration date
• Offers access to higher Levels of Assurance

• Required:
  ▪ Protect user's private key
  ▪ Assure uniqueness of certificate across CA domain namespace
  ▪ Provide central revocation method

• Optional:
  ▪ Add attributes (groups/roles) as extensions to cert
    – From VO: (e.g., VOMRS roles and groups)
    – From IdP: (e.g., faculty or student membership)
How Can Campus IdM Use Benefit a Grid User?

• By simplifying resource requests
  - Leverage existing IdM data to automate much of registration authority (RA) function
  - Maintain list of unique Distinguished Names (DNs)
  - Identify problems requiring human intervention

• By facilitating VO role management and private key protection
  - Example: Require Level of Assurance "2"
    - as defined by Federal e-Authentication standards
  - Example: use Shibboleth sessionID as high-entropy private key
  - Define VO attributes and roles as X.509 certificate extensions or by SAML assertions from a VO attribute server
• **AUTHENTICATE** Identity
  - Does IdP know this user based on in-person ID vetting?
  - Request user attributes from IdP.
    - If `eduPersonEntitlement "Peligible"` attribute is asserted, enable "Request Allocation" button
  - Query TACC Accounting DB for User Context
    - Check that user answers security question setup at initial registration
    - Check for active Projects, Allocations, and VO membership and roles
    - Find user's unique Distinguished Name (DN) by querying DN list by `eduPersonPrincipalName` and initial registration date
  - Query VO attribute server to verify user's VO membership and roles
    - Determine length of short-term certificate
  - Enable "Get short-term X.509 cert" button

• **PROVIDE** resulting short-term X.509 credential where user wants it
Example: 1) Grid Portal Authentication

Supports Portal Login
OR
Shibboleth Login
2) UT-System Shibboleth WAYF Dialogue

User Selects Identity Provider from Pull-down menu

In order to fulfill the request for a web resource you have just attempted to access, information must be obtained from your home institution. Please select the institution with which you are affiliated.

Select your home institution

Choose from a list:

- University of Texas System Administration
  - Select
  - Remember for session

or

Search by keyword:

Search

Need assistance? Send mail to UT System IDM Support with description.
3) Authenticate with Home Identity Provider

Regular Campus/IdP login.
This one is for UT-System
Each IdP Presents Its Own Dialogue/Look and Feel

You are entering a Secure Service - please log in!

UT EID: Help for job applicants.
Password: Help for prospective students.

Quick Password Change and Login.
Forgot Your Password?

This is the login dialogue for the UT-Austin IdP
ProtectNetwork offers both free LoA-1 identity and Validated LoA-2 identity for $$.

(One option for external, low-risk application users.)
Attributes contain user and IdP info.

Attribute Release Policy controls which attributes get released to each application.

Attributes can be pushed or pulled.
• NMI-EDIT "Extending the Reach" Grant
• Shibboleth Install-fest held
• Policies and procedures documents written
  ▪ Charter, Member Agreement, FOP, MOP, Attributes, Fees at https://idm.utsystem.edu/utfed
• Production Federation formed
• Eight federated applications currently in production (and several more in development throughout the system)
• Pursuing discussions with other parties interested in Identity Management system inter-federation.
SURAggrid Two-tier PKI strategy

Jerry Perez
Research Associate
TTU High Performance Computing Center
Introduction to SURAgrid

- Started as NMI Testbed Grid project in 2003.
- Organized by the Southeastern Universities Research Association (SURA).
- Now extends across many participating universities and institutions.
- Bridge CA for trust relationship developed by Jim Jokl, University of Virginia, lead for AuthN/AuthZ development.
- Used within the SURAgrid computing effort.
• SURA Bridge CA cross-certifies participating certificate authorities (CA's)
• Secure process for submitting certificate signing request (CSR), usually at F2F meetings
• Participating CA's must conform to specific OpenSSL constraints
• Central SURA repository for signed CA certs
• Actual bridge CA machine is offline
• Details at https://www.pki.virginia.edu/sura-bridge/
• AuthZ via SURA LDAP server
• Central LDAP server used for storing grid-mapfile and user login info (username, institution, uid, gid, home, email)
• Administrative web interface to add users
• Rudimentary Perl scripts to grab grid-mapfile and login info. Easy customization.
• Secured by trusted SSL cert – enable SSL cert verification in Perl scripts on client.
• Note some institutions do not permit external LDAP server to be used directly (see next section).
• One of two bridges proposed for use in higher ed.
• Higher Education Bridge Certification Authority (HEBCA).
• Trusted electronic communications within and between institutions of higher education.
• Federal and state governments are included.
• Modeled on the Federal Bridge Certification Authority (FBCA).
• Allows a complex collection of institutions to share trusted electronic credentials necessary for a broad range of applications in education, research, and administration.
• The US Higher Education Root (USHER) is a public key infrastructure (PKI) supported by the higher education community.
• Relies on a simplified common policy framework and self-accreditation.
• Operated by the USHER Policy Authority and Internet2.
• Supports emerging deployments in research, education, and transactions in higher education that require PKI.
Two-Tiered PKI for SURAgrid

• Goal is to provide security within the present collaborative environment.
• Prepare for the future: federated security infrastructure combining campus ID management with integrative components and services from higher education, federal and perhaps commercial sectors (e.g. HEBCA, FBCA, IGTF).
Multi-Level Access within SURAgrid

- SURAgrid Bridge joins together two different tiers defining Levels of Assurance (LoA).
- First tier operates at a local level in which sites generate their own X.509 certificates that are trusted across SURAgrid. This is good for local collaboration (primarily southeastern region of the United States).
- Second tier operates at a higher level so that certificates meet IGTF requirements and LoA’s at a national level. This is good for interoperating with other grid initiatives such as TeraGrid, Open Science Grid, and TIGRE.
- Participating in Bridge Working Group of the IGTF.
- The assumption is that HEBCA will emerge to become the longer-term trust fabric for SURAgrid.
Next Steps

- Integrate SURAgrid AuthN/AuthZ into project common software stack to be selected.
- Resolve institutional boundary issues.
- Complete two-tier PKI deployment.
- Pursue integration with AuthN/AuthZ systems used by other grids (see next talk).
IdM Tools for Grids

Alan Sill, Ph.D
TIGRE Senior Scientist
TTU High Performance Computing Center
Grid Standards Framework

• Grid application software and middleware are developed by many different groups.
• Standards essential to the success of the process.
• Grid standards are primarily developed within the context of the Open Grid Forum (OGF). OGF was formed by a merger of the previous Global Grid Forum (GGF) and the Enterprise Grid Alliance (EGA, an industry-based grid organization).
• Current efforts are focused on the Open Grid Services Architecture (OGSA) and other activities within OGF.
OGF and Related Groups

- OGSA-AuthN: focused on authentication (new group currently being formed).
- OGSA-AuthZ: authorization standards.
- International Grid Trust Federation (IGTF): a separately chartered group focused on accreditation of identity providers for grid authentication.
- CA-Ops: Certificate Authority Operations; best practices interface between OGF and IGTF.
Identity is communicated in the context of the Grid Security Infrastructure (GSI) and established via exchange of X.509 certificates using PKI.

Efforts are also in progress on many fronts to make use of SAML-based exchange of cryptographic information to leverage campus-based federated IdM systems.

Username/password access is deprecated outside of the context of integration with a secure IdM system, and primarily limited to access to low LoA applications.

Multi-factor and high LoA systems being studied.
• LoA Research Group (RG) formed as a result of efforts at the last OGF meeting (OGF-19).
• Will study and advise OGF on methods to incorporate LoA observation and transmission within the context of grid software.
• Essential to progress in certain fields.
• Will be useful for improving ease access to portals and science gateways as well as to establishing communication standards for protecting high LoA applications.
• OGSA-AuthN charter effort in progress to provide a formal mechanism for extending grid standards to include federated identity.
• Charter Birds-of-a-Feather session held at OGF-19.
• Note this is an extension from previous grid security authentication efforts and not a green-field start.
• Must take into account existing grid service authentication practices as well as extensions to the future.
• Participation welcome: ogsa-authn-bof@ogf.org
The International Grid Trust Federation was formed beginning in 2003 and officially launched in 2005 at GGF-15.

- Responsible for accrediting grid identity providers.
- Membership consists of Certificate Authorities organized into 3 regional Policy Management Authorities (PMAs) across basically time-zone boundaries in the European, Asia-Pacific and Americas regions.
- The Americas Grid Policy Management Authority (TAGPMA) operates in the North, South and Central Americas region.
• TAGPMA includes members from Canada, the US, Mexico, Venezuela, Argentina, Chile and Brazil.
• Meet 3 times / year to review requests for accreditation and other related business.
• Several new CA’s within the US, including ones related to Teragrid.
IGTF Activities

- PMAs comprising the IGTF have created several authentication profiles to cover “classic X.509” PKI, short-lived credential services (SLCS) based on Kerberos-like secure infrastructures, a membership-integrated credential service (MICS) in development to leverage general campus/institutional IdM systems, and an experimental profile.
- Roughly 80 CA’s throughout the world have been accredited; some operate more than one such accredited service.
- This system forms the backbone of the identity management used by large-scale international grids.
• Authentication (establishment of identity) is distinct from local authorization in most distributed-access grid and similar systems.
• AuthZ is handled by many different software packages and systems that leverage identity tokens provided to them, primarily by strong-authentication SAML or PKI tokens.
• Local AuthZ and the decision of what CA’s or identity providers to trust is always a local decision.
• Example: TIGRE provides and uses X.509 credentials but leaves local account mapping and authorization to the participating institution.
• In the Open Science Grid, EGEE and other large-scale projects, Virtual Organization Membership Services (VOMS) software is used. Management is often supplemented by a Registration Services system known as VOMRS.

• Different projects use differing software on the computing or storage resource to access and obtain user-oriented VO information from the VOMS server.

• Activities are increasing to develop VO server equivalents and/or access methods to use VO-based attribute information in the context of Shibboleth and other federated IdM systems.
• Using TACC-supplied CA - new version recently accredited by the IGTF.
• Local AuthZ based on grid-mapfiles and/or GUMS/PRIMA implementation (optional so far).
• Compatible with AuthN/AuthZ approach used by Open Science Grid, LCG, EGEE, etc.
• Looking at methods to read SURA LDAP information to be used as a factor in local AuthZ and account mapping decisions.
• Will work with UT and other participants to integrate where possible with Shibboleth and other local IdM systems.
Thank you!

- For more information, please contact:
  - Paul Caskey  pcaskey@utsystem.edu
  - Marg Murray  marg@tacc.utexas.edu
  - Jerry Perez  jerry.perez@ttu.edu
  - Alan Sill  Alan.Sill@ttu.edu
Copyright Notice

Copyright Paul Caskey, Margaret Murray, Jerry Perez and Alan Sill, 2007. This work is the intellectual property of the authors. Permission is granted for this material to be shared for non-commercial, educational purposes, provided that this copyright statement appears on the reproduced materials and notice is given that the copying is by permission of the author. To disseminate otherwise or to republish requires written permission from the authors.