Authentication Project Report

“Simplified Access to Computer Systems”

Stuart Anderson for AuthProject
Warren Anderson (Co-chair)
Dave Barker
Sam Finn
Scott Koranda
Jeff Minelli
Tom Nash (Co-chair)
Shannon Roddy
Diego Menéndez
Hannah Williams

The Challenge

- Almost every connection to a LIGO web client, computer, grid, console, …, involves:
  - » A different user name
  - » A different password
  - » A new log-in session
  - » And a different protocol
- Inefficient and confusing for both new and long time users.
- Major time drain for those who support computing and those trying to gain access.
- Contributes to loss of science opportunity and security concerns.

The Goal

Maximize science and minimize security barriers and hassles

"login once at the beginning of the day and then forget about passwords"

Characteristics of a New Approach

- Enable rapid access to all access controlled computational resources by new community members.
- Remove the need for a “dozen secret handshakes”, by providing one user name/password pair per user.
- Reduce the usage costs (backend support and end user) through centralized maintenance of secrets.
- Facilitate working group communications through decentralized and self maintained membership tools.
- Reduce the number of security technologies that users must understand, e.g., certificates.

Three Environments

- Web services (web pages, wikis, ilogs, cvs, ...)
  - » Prompted for single login on first access to a web site
  - » Eventually support changing between sites without re-logging in
- Data Grid and Clusters for analysis
  - » Same login name/password automatically generates temporary certificate from central repository
    - – No need to apply for certificate (part of joining community)
    - – No need to renew certificate each year
    - – No need to learn how to “keep it secret, keep it safe”
- Workstations and Consoles
  - » Same login access as above will grant seamless access to interactive logins

The Benefits

- New members
  - » Drastically lower barriers to getting started on your science, “days become hours”.
- Community wide
  - » Only one password to remember.
  - » No more renewing certificates: remembering how, finding & discarding old ones, downloading and installing new one.
  - » Less time lost when things don’t work & you can’t access something quickly.
- Grid management
  - » Reduced time spent supporting user problems and confusion with certificates.
- System administrators
  - » Common support for access controls.
- Website managers
  - » No need to manage local access controls unless desirable.

Continuing Benefits

- Working group chairs
  - » Easy to set up and maintain group lists and access controls
- Principle Investigators
  - » The same list you maintain for authorship and shift taking will be used for access control for your group.
  - » Automatic creation of credentials to allow access by new group members when you first add them to the Roster.
- Collaboration leadership
  - » No more common passwords which get compromised and need to be replaced.
  - » Easy to set up and manage committees

The Work

- AuthProject
  - » Upgrade Directory Services
  - » Complete configuration and deployment of core services
  - » Document instructions for web and system managers
- Web Managers
  - » Switch to new standard authentication modules
- Sys Managers
  - » Switch authentication and authorization modules
- Collaboration and working group leadership
  - » Establish working group authorizations via new group management tool
- Community
  - » Remember and protect your personal ligo.org password
  - » Sign up to help integrate your favorite tool sooner rather than later, see task chart on AuthProject wiki (link from demo.ligo.org)

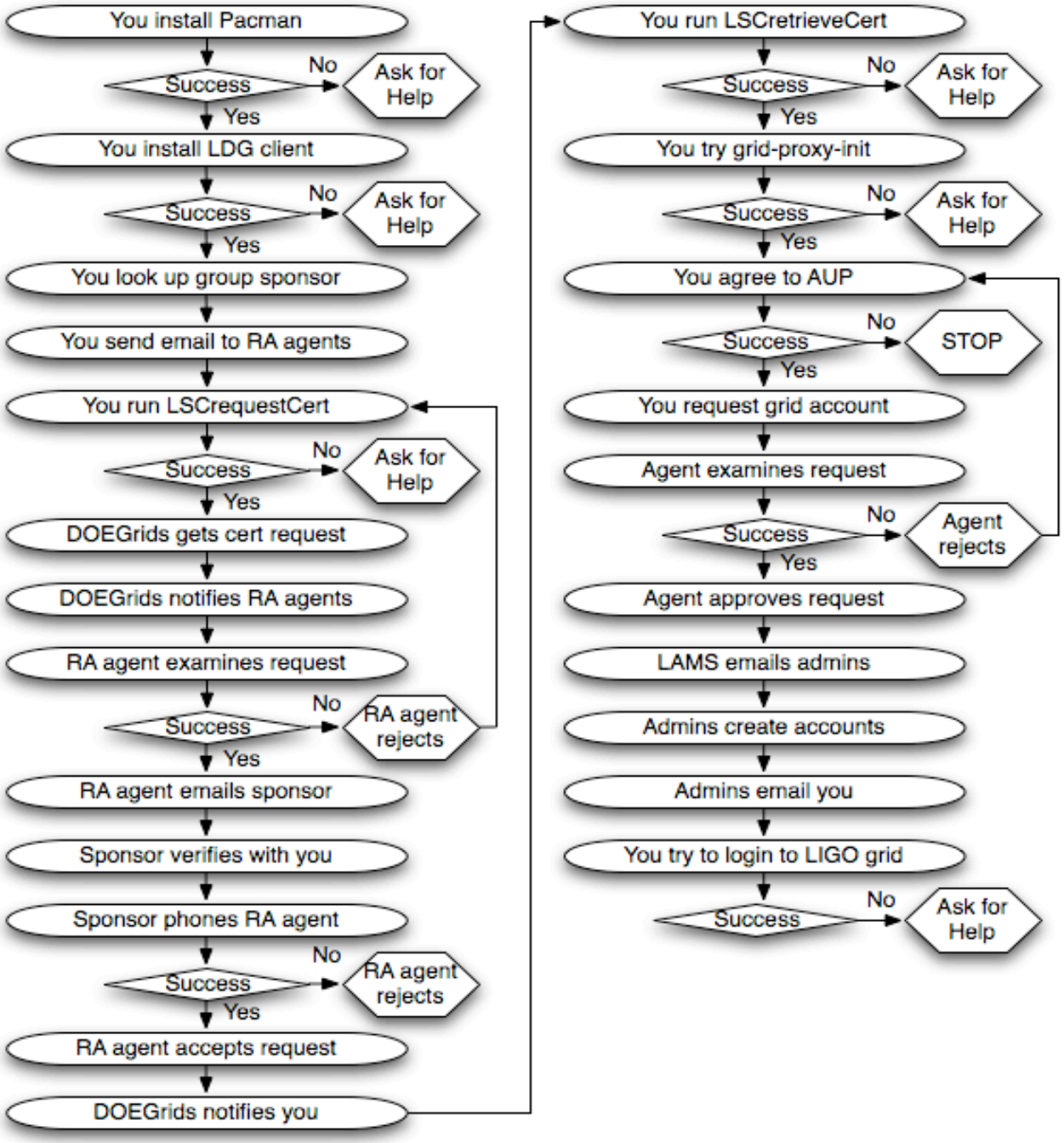
Current Status

- Individual pieces of the solution identified and tested.
- Some services (e.g., web) ready to go live with common sign on functionality.
- Production wiki up and running for AuthProject, http://demo.ligo.org. This wiki has links to other initial production systems:
  - » Additional types of wiki's (Twiki, MoinMoin, and MediaWiki).
  - » Bug tracking system (RT).
  - » Simple static web site (LIGO S5 sensitivity curves).
  - » Task chart showing in detail the remaining steps with level of effort estimates. Note, many parallel few day tasks to sign up for.
- CompComm web site managed by these tools.
- Services can be rolled out individually and you will simply start using your ligo.org login name for more and more systems.

The End of the Beginning

- Please visit demo.ligo.org and select “AuthProject”.
- Please talk to us now about your concerns and priorities for integrating new services.
- Many tools have multiple integration solutions, please sign up to integrate your favorite tool.

- Current grid certificate process!!!
- 1/4FTE to support.
- Typically 1 or more interesting problems.



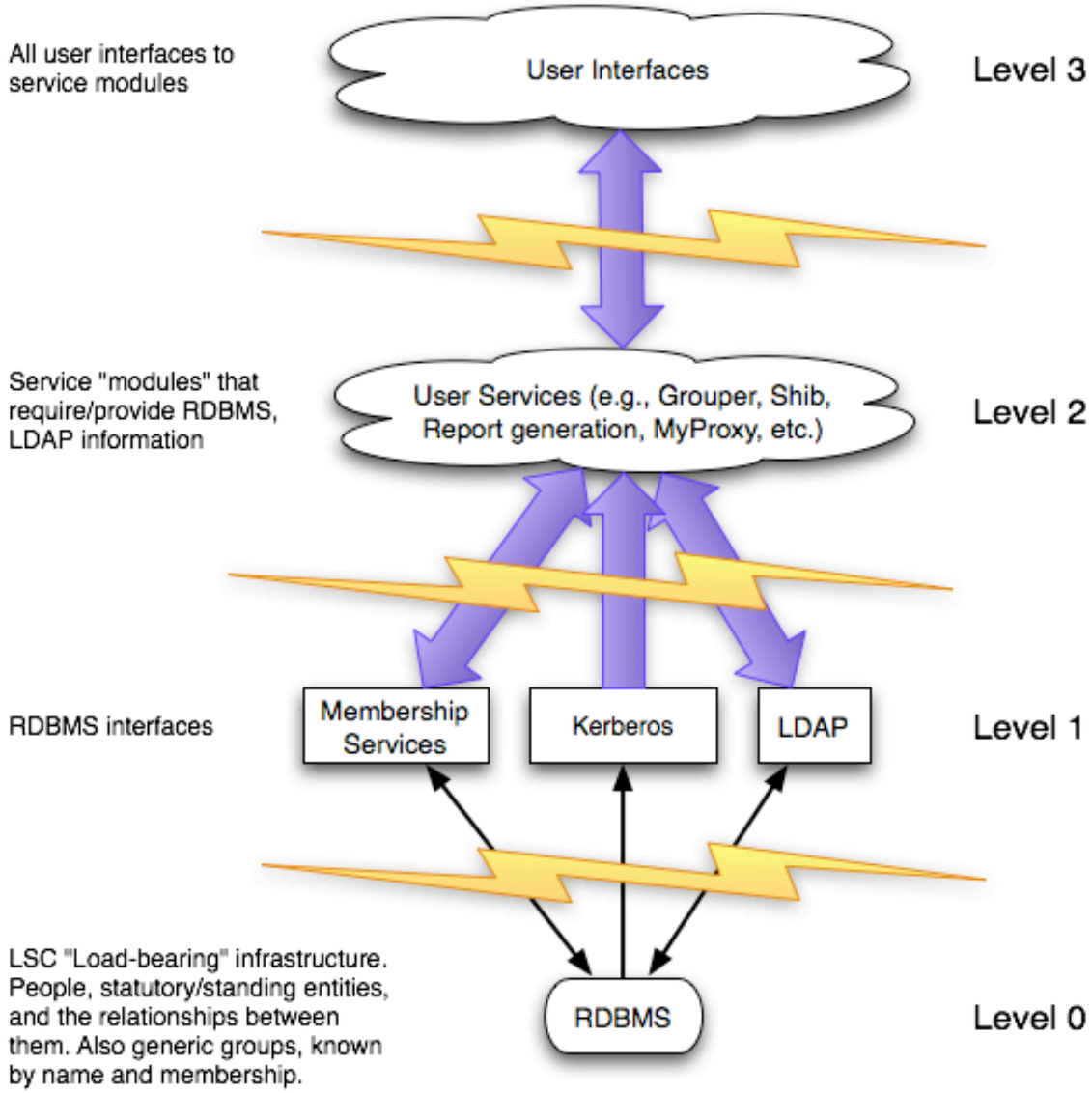
Universal Single Sign-on

- Authentication: establish your identity.
- Authorization: permits you to access a resource.
- Single password: your password works for all accesses that are a part of the new regime.
- Single sign-on: you authenticate on your workstation, console, laptop, ... once per day or session.
  - » automatic log-in to all resources for which you are authorized for the rest of the day: compute clusters, wikis, websites, ilogs, CDS gateways, workstations, …
- More robust, easier to manage and use.
- Increased security and better control of who has access to what.

Underlying Tools

- Kerberos
  - » Main authentication tool using symmetric cryptography.
  - » Standard tool on a very large list of platforms.
- Shibboleth
  - » Internet2 tool for single sign-on to web services across multiple domains.
  - » many services already “Shib-aware”, others easy to adapt.
- MyProxy
  - » central storage and management of user X.509 certs.
  - » accessed via ligo.org kerberos credential and single sign-on.
  - » Issues temporary proxy certificate that does not need to be managed.
- LDAP
  - » **L**ightweight **D**irectory **A**ccess **P**rotocol (LDAP).
  - » PAM Kerberos authentication a default capability of most OSes (*nixes).
  - » LDAP unix account information then used for console or ssh authorization.
- Directory Services
  - » ligo.org roster is SQL database for collaboration management tools.
  - » new members, change of passwords, author lists, LSC MOU Att. Z.

The Architecture



History

- The LSC Computing Committee was convinced that the current ad hoc approach of adding new services with differing authentication and authorization systems was too complex to maintain and scale as both the LSC and the number of network services was projected to grow.
- Authentication & Authorization Sub-Committee formed in early 2007.
- AuthProject developed universal LIGO single sign-on plan,

  LIGO-T080058-00-U
- Prototype models demonstrated at the March 2007 L-V meeting.
- LSC Directorate approved project in fall 2007.
- Status: now ready for early production use

  ... and ready to tell you what this is all about

Authorization Tool

- Grouper is simple web-based tool to:
  - » create and manage group attributes.
  - » create working group lists, committees, access control lists, ...
  - » basis for access authorization to websites, computers, ...