GFD-I.079
Individual submission

Von Welch, NCSA
March 6, 2006

Report for the GGF 16 BoF for Grid Developers and Deployers Leveraging Shibboleth

Abstract

This document summarizes the BoF held across two 90 minutes sessions at GGF 16 in Athens for Grid developers and deployers leveraging Shibboleth.

Contents

1 Overview

This document summarizes the Birds of a Feather (BoF) sessions held at GGF 16 on February 14th and 15th in Athens, Greece. The event consisted of two 90-minute sessions, one on each day. The first session consisted of a series of talks by various Grid developers and deployers who were interacting with Shibboleth, as well as a presentation of upcoming Shibboleth plans. The first session had roughly 50 participants and the second session had roughly 40 participants.

Activities in the area of Shibboleth will continue in the form of an email list created for this activity: “shibgrid-bof@federation.org.au.” To subscribe visit: http://www.federation.org.au/cgi-bin/mailman/listinfo/shibgrid-bof

The goal to form a federation testbed to test interoperability among the various projects was agreed to at the meeting, with a rough timeframe around GGF 18. Details will be discussed on the aforementioned email list.

This document assumes readers are familiar with Grid security concepts, technologies and terminology. Readers unfamiliar with Shibboleth may find more information at the Shibboleth project web page: http://shibboleth.internet2.edu/

2 Session One Speakers and Talks

The first session, on February 14th, consisted of eight individual presentations. This section contains the agenda for the first session and brief summaries of the presentations. Slides are available online at the following URL:

http://www.ggf.org/gf/event_schedule/index.php?id=213

The agenda for the first session was:

- Andrew Martin - Oxford/CCLRC `ShibGrid' project
- Erik Vullings – “A Ship on the Grid”
- David Chadwick - GridShibPermis
- Mike Jones - SHEBANGS/Shib and Shibboleth integration into GridSite
- Christoph Witzig - SWITCH
- Richard Sinnott - NeSC Glasgow activities
- Von Welch - GridShib/MyProxy
- Nate Klingenstein - Shibboleth 2.0 plans

A summary of project timelines is as follows. The suggestion was made to gather more detailed deliverable timelines on the email list to help projects make plans for leveraging each other.

- Shibboleth 2.0 – Beta in May/June ’06; Final release end of summer.
- Shibboleth 2.1 - ‘07
- SWITCH - EGEE2 April ‘06-March ’08 (three phases, see summary)

- SHEBANGS - Ending Feb ‘07
- SHIBGRID - Ending Feb ‘07
- GRIDShib - Ending Spring’07
- MAMS - Ending ‘06
- Shibboleth integration into GridSite, PERMIS – to be released soon
- DyVOSE/GLASS/VOTES - Ending Feb ‘07

2.1 Andrew Martin - Oxford/CCLRC `ShibGrid' project

Andrew Martin opened the presentations with a description of the JISC-funded “ShibGrid” project at Oxford/CCLRC. This project, scheduled to being work on March 1st, 2006, and last for one year, has the goal of integrating the National Grid Service (NGS) into the academic framework. The project will develop a prototype system that will allow NGS users to access NGS facilities securely through the Shibboleth authentication framework. The project has two target user communities: e-Diamond and Integrative Biology

The project will begin with requirements gathering, looking at allowing users, both who have and do not have certificates, to access NGS via Shibboleth. The project will consider three scenarios:

1. User’s only credentials are Shibboleth provided. A user would authenticate to an online CA to gain an X.509 proxy certificate, which would be created with a DN obtained from a Shibbolth issued attribute, via a “shib-proxy-init” application. Andrew mentioned it would be desirable to do with a command-line client, but there doesn’t seem to be any means of doing so without customizing the client for each Shibboleth IdP.
    a. A variant of scenario 1, but the user has a long-term certificate in credential store.
2. The user registers with NGS using a web form, uses Shibboleth to present a DN to NGS’s existing DN-based authorization system.
3. Enhance the NGS portal to use Shibboleth for access control.

2.2 Erik Vullings – “A Ship on the Grid”

Erik Vullings gave a presentation of the Meta Access Management Systems (MAMS), an Australia-based project. This project, which started in 2004, has a scope much larger than Shibboleth and Grid and was founded to provide identity management solutions to several other Australia projects. Erik described prior and current work of the MAMS project, including creation of a InQueue-like federation, with a CD for easy installation, Shibbolization of GridSphere, DSpace, Zope/Plone, and Wiki, and work with XACML (including a XML-free XACML editor) for authorization to repositories.

Erik described efforts to enable an authenticated federation search (AFS) service that would allow a search through multiple repositories through a single federated interface. Assuming each repository was Shibboleth-enabled, this would require a mechanism to allow for Shibboleth-enabled access to the AFS service and delegation to that service for access to the federated services it represents. Erik described a scheme to allow this (see slide 9) by having the user perform Shibboleth authentication to the AFS service, then having the AFS create a session via the Shibboleth IdP to the federated services and then using that session for querying the services.

Erik also discussed work to enable Shibboleth access to MyProxy, using a similar session-based scheme as described for AFS access. A claim transformation service (CTS) was also described that acts as an aggregator and translator of attributes for VO users (in a similar manner to myVocs, which was developed in parallel). ShARPe, a tool developed to provide users with a GUI for managing their Shibboleth attribute release policies (ARPs) was also presented.

(Editor's note: Erik's presentation included a slide representing the middleware landscape based on Tolkien's middle-earth that is worth looking at.)

2.3 David Chadwick - GridShibPermis

David Chadwick presented work with integrating PERMIS into a number of other Grid components to provide a policy-based authz infrastructure. This included plugging PERMIS into GT 3.3 (via the GGF OGSA-Authz callout), into a Shibboleth SP to provide access control decisions based on Shibboleth attributes as well as X.509 attribute certificates (replacing mod_shibauthz with mod_permis; this work is effectively integrated PERMIS with plain Apache as well), into GT4 (again with the OGSA-Authz callout) and integrated, directly via a Java API, into GT4 and GridShib (not released yet due to Java bug with the cryptography libraries).

2.4 Mike Jones - SHEBANGS/Shib and Shibboleth integration into GridSite

Mike Jones described two separate projects. The first is the recently-funded SHEBANGS project. SHEBANGS, like the ShibGrid project as presented by Andrew Martin, has a similar goal to allow Shibboleth-based access to NGS, but with several key differences including a focus on Portals, an integration with VOMS and a starting assumption that many users do not possess any X.509 credentials.. Their plan is to develop a credential translation service (CTS, not to be confused with the CTS as described by Vullings) that would produce Grid credentials based on Shibboleth authentication and place those credentials into MyProxy for future access by the user to NGS. CTS would also integrate with VOMS by gathering attributes from VOMS and embedding those into the credentials it places in MyProxy.

Mike also presented a conceptual complex VO structure based on CTS and a "Which VO are you from" (WVOAYF, see slide 9) that would allow a VO to aggregate IdPs representing its users.

The second part of Mike's talk presented work by Andrew McNab and Joseph Dada on integrating Shibboleth into GridSite using a scheme that created a password-protected DB entry that contains the user's DN. This DB entry would then be served with a Shibboleth IdP to SPs, providing the DN as an attribute and allowing for DN-based access control. Future work includes XACML-based access control and integration with VOMS.

2.5 Christoph Witzig – SWITCH

Christoph Witzig begin his presentation by reminding us it was Valentine's day (a bit too late for the Australians). He then presented plans by the Swiss Education and Research Network for Shibboleth and Grid. SWITCH currently has the SWITCHaai, a national infrastructure for authentication, authorization and identity based on Shibboleth, which has 133k users (10k regular users). SWITCH also operates a national PKI (using a commercial CA).

As part of their participation in EGEE-2, SWITCH is working on interoperability between Shibboleth and gLite. Their goal is to integrate existing code, doing development only as needed. Their model is one where the user's home institution provides the user's identifier through a Shibboleth IdP and the VO contributes user attributes.

Work will begin in April of 2006, and last 2 years. There will be 2 initial short phases in the summer and fall of '06 in which they will achieve interoperability between their Shibboleth-based AAI infrastructure and gLite grid with minimal changes (in particular to the compute element). Phase 1 will involve generation of short-lived Grid credentials from a Shibboleth-authenticated certificate service. Phase 2 will add attribute retrieval from VOMs. A longer 3rd phase will commence in the fall of '06 with the goal of adding SAML support to the end Grid resources. The detailed design of this third phase will be done during the summer of '06. It is planned that this work will be based on Shibboleth2.

2.6 Richard Sinnott - NeSC Glasgow activities

Richard Sinnott described a number of existing and planned uses of Shibboleth in Grid deployments.

DyVOSE provided an advanced authorization infrastructure for education using GT 3.3 and PERMIS. An IdP was deployed to represent project membership.

BRIDGES provided a portal that used Shibboleth to authenticate and authorize users and then used a local service certificate to submit BLAST (and only BLAST) jobs to the Grid.

VOTES (VO for trials and Epidemiological Studies), plans to develop a Grid infrastructure to address key components of client trials and observational studies. Shibboleth will be used to provide access control to queries to the VOTES statistics database.

GLASS (Glasgow early adoption of Shibboleth) is a JISC-funded project that will start in March of '06. It will build on an existing university account management system and will look at providing secure access to brain trauma patient data from the Glasgow Southern General Hospital.

2.7 Von Welch - GridShib/MyProxy

Von Welch presented prior and planned work of the NSF-funded GridShib project. Work to-date, publicly available from the project web page, has been focused on the access to the Shibboleth attribute authority by the GT4 through the development of plugins to the Shibboleth IdP to recognize DNs and enhancements to GT4 to obtain attributes and make access control decisions based on those attributes.

Future work includes refinement of the attribute access work, including the development of a service to bind user's Shibboleth identifiers to Grid DNs, and the use of Shibboleth for single sign-on to the Grid. He gave a URL for a prototype "SP-CA" that issues short-lived credentials to the user based on Shibboleth authentication and uses Java Web Start to move the credentials to the user's desktop.

2.8 Nate Klingenstein - Shibboleth 2 plans

Nate Klingenstein from Internet 2 presented the Shibboleth developers plans for upcoming Shibboleth 2.0 and 2.1 releases. He started with a discussion of new features available in the SAML 2.0 specification and plans for the development of OpenSAML.

Shibboleth 2.0 will mainly provide similar functionality to Shibboleth 1.3 based on SAML 2.0, with a few enhancements: including authentication integrated into the SSO, a Java SP, improved SP clustering and a production-ready WAYF. An initial beta will be available in the May/June '06 timeframe with a final release around the end of summer.

Shibboleth 2.1 will additionally include delegated authentication, account linking, attribute aggregation, enhance client support, global logout and improved targetedId support. The timeline for 2.1 is not set at this time.

3 Day Two Discussion Session

Von Welch led discussions during the second session. The various topics are captured here, organized by sections. The slides from day 2 are available at:

http://www.ggf.org/GGF16/materials/Grid%20Shib%20Bof/shib%20copy%208/ggf16-shib-bof-day2.ppt

3.1 Discussion of Common Areas

Von started with his observations of some common areas of mutual interest across the projects to spur conversation of possible collaboration.

- Short-lived X.509 credentials from Shib authentication: ShibGrid, SWITCH, SHEBANGS, GridShib
- Access to user DN via Shib AA: ShibGrid, Shibboleth integration into GridSite
    - GridShib is working on name binder which seems related
- Shibboleth authentication to MyProxy: MAMS, SHEBANGS, GridShib
- N-tier problem/ Shib-Portal-Grid (seem related)
    - MAMS
    - VOTES/GLASS, ShibGrid, MAMS, SHEBANGS
- VO Services: MAMS, SHEBANGS
- VOMS Integration: SHEBANGS, Shibboleth integration into GridSite, SWITCH

3.2 Internet2 April Member Meeting

A 90 minute session has been scheduled at the upcoming Internet2 member meeting on April between Shibboleth developers and Grid developers/deployers. This session is opened to anyone from the Grid community who is interested. Von suggested that the group could come up with a common set of requirements and/or requests for the Shibboleth team.

3.3 Potential Topics for Group Work

The group discussed a number of potential topics of common interest that could be worked on by the group:

- Draft requirements document for April 24th I2 Meeting
- Definition of a VO and how one would architect a VO in Shibboleth
- VOMS/VO management interop
- VO-VO federation
- Shib/Grid portal architecture
- N-tier/delegation
- How to map Shibboleth/Grid names
- Anonymity
- IdP discovery
- Specific attributes useful for Grids
- Institution vs VO maintained information
- Authentication methods
- Test federation among projects
    - Identify users; ties to GIN

3.4 Next Steps

The following next steps were agreed to:

1. Von will work with GGF to create an email for further discussions. The list will be advertised on security-area@ggf.org, shib-users email list, Workshop page, and Erik's page: (http://tinyurl.com/bmsnn). Folks can also send email to Von (vwelch@ncsa.uiuc.edu) to receive notification of the creation of the email list.
2. The list will be open to discussion of any of the topics identified as possible next steps, or other topics related to Grid and Shibboleth. Based on what discussions occur between now and the next GGF, a research or working group could be formed with a charter based on the conversations that emerge.
3. The suggestion for a federation testbed between the various projects was proposed and there was general agreement that this was a good idea. A rough target of the fall GGF seemed reasonable. Details will be decided on the list.

4 Security Considerations

Many of the presentations at the BoF focused on security, however the presentations should be taken as opinions of the presenter and are not recommendations of any GGF working group.

5 Project URLS

More information on the various projects presented can be found at the project web sites listed below.

- ShibGrid: None available at this time, a link will eventually be available from http://e-science.ox.ac.uk/
- MAMS: http://www.melcoe.mq.edu.au/projects/MAMS/
- PERMIS: http://www.permis.org/
- SHEBANGS: http://www.sve.man.ac.uk/Research/AtoZ/SHEBANGS
- GridSite: http://www.gridsite.org/
- SWITCH: http://www.switch.ch/
- DyVOSE: http://labserv.nesc.gla.ac.uk/projects/dyvose/
- GLASS: http://labserv.nesc.gla.ac.uk/projects/glass/
- VOTES: http://labserv.nesc.gla.ac.uk/projects/votes/
- GridShib: http://gridshib.globus.org
- Shibboleth: http://shibboleth.internet2.edu/

6 Acknowledgements

The editor wishes to thank the GGF staff and the Security area directors for helping to facilitate this event on relatively short notice.

7 Author Information

Von Welch, Editor
NCSA
vwelch@ncsa.uiuc.edu

8 Intellectual Property Statement

The OGF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the OGF Secretariat.

The OGF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this recommendation. Please address the information to the OGF Executive Director.

9 Full Copyright Notice

This document and the information contained herein is provided on an “As Is” basis and the OGF disclaims all warranties, express or implied, including but not limited to any warranty that the use of the information herein will not infringe any rights or any implied warranties of merchantability or fitness for a particular purpose.