

GPN Annual Meeting 2010

***Fault Tolerant and Highly Available  
Entitlement Server for CI  
Collaboration***

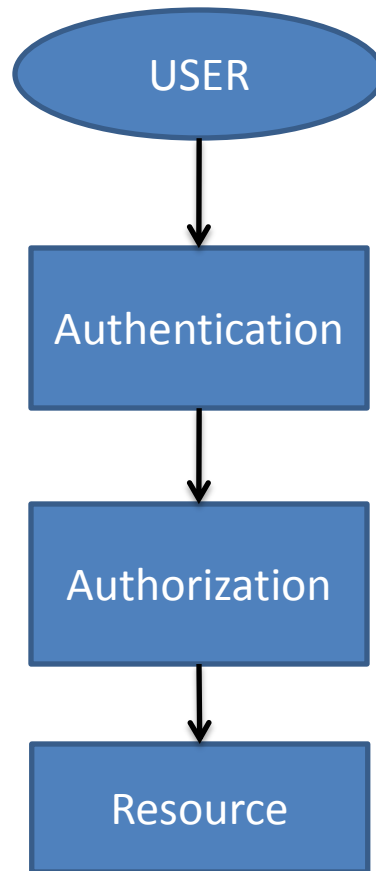
By

Harcharan Singh<sup>1</sup> and Gordon K. Springer<sup>1,2</sup>

Computer Science Department<sup>1</sup> &

MU Informatics Institute<sup>2</sup>

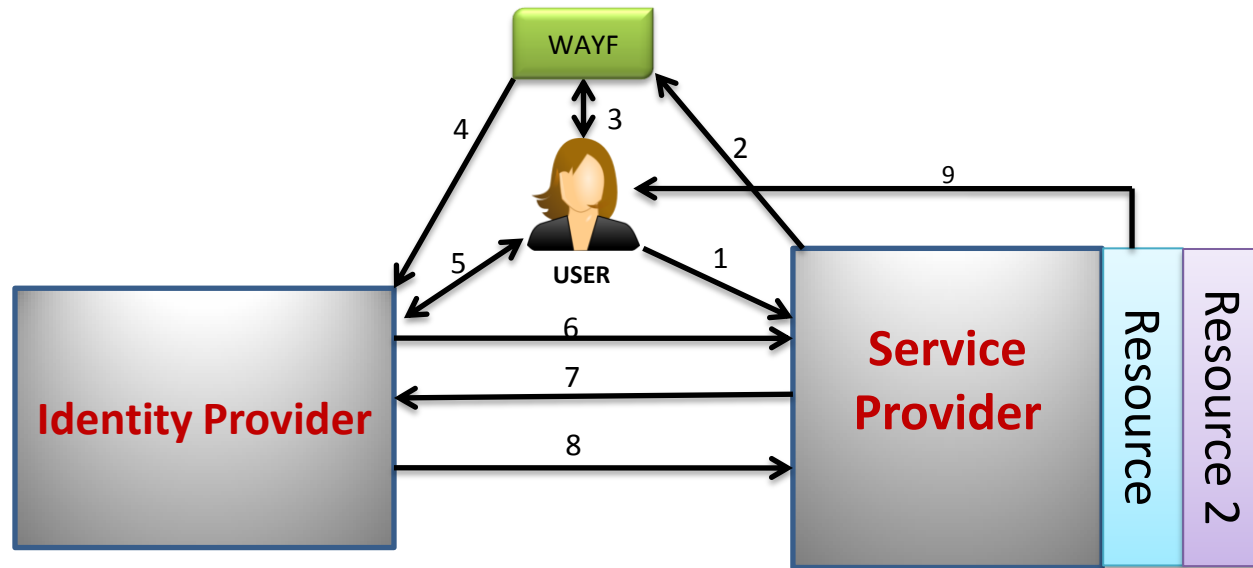
# Standard Mechanism to Access restricted computing resource



# Shibboleth Architecture

- Shibboleth is an Internet2 standards-based architecture used to support sharing of computing resources.
- Shibboleth is middleware initiative that offers a mechanism to authenticate and authorize user's in federated environment.

# Shibboleth Federated Environment



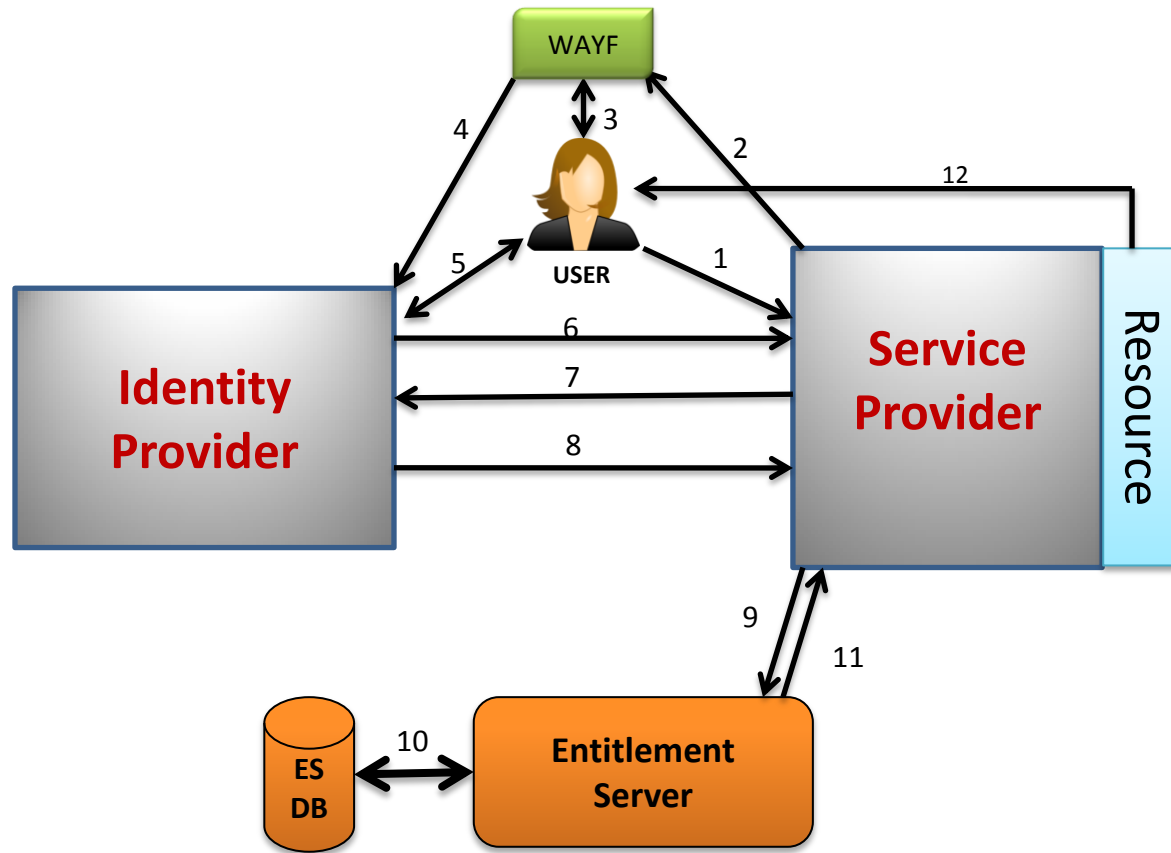
# Virtual Organization

- A virtual organization is an umbrella organization that includes all the research institutions that share a common goal.
- Provides the member institutions with secure and robust inter-institutional collaborative research environment

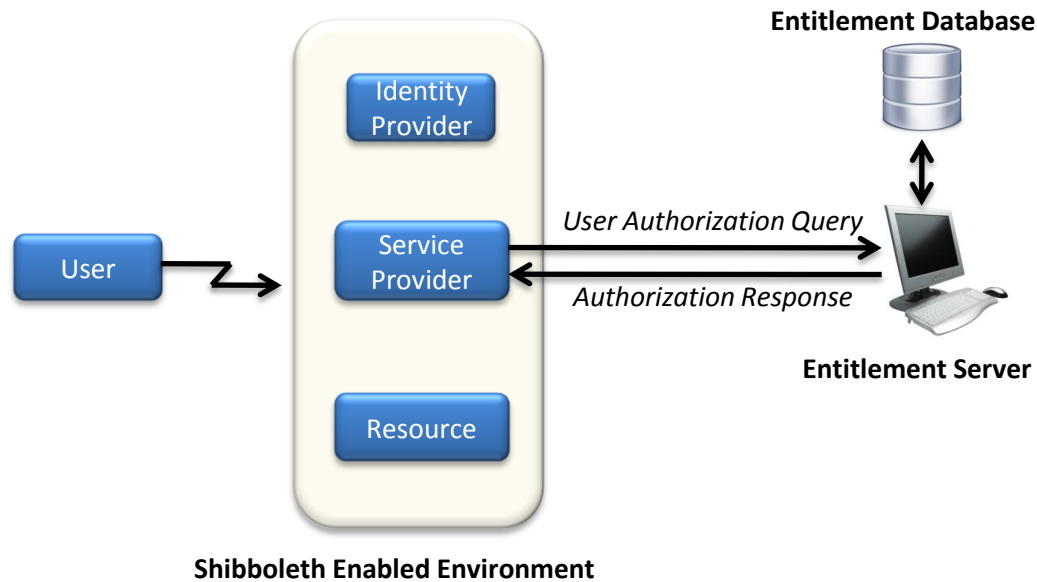
# Entitlement Server

- Defines, manages and uses virtual organization entitlements independent of any institution
- Fine-grained authorization using data that may not exist in an Identity Provider E.g. name of the Virtual organization that the user belongs

# Shibboleth Federated Environment including Entitlement Server



# Authorization process using Entitlement Server



“Does the user have the “urn:mace:greatplains.net:biogrid” entitlement?”

“yes” or “no”

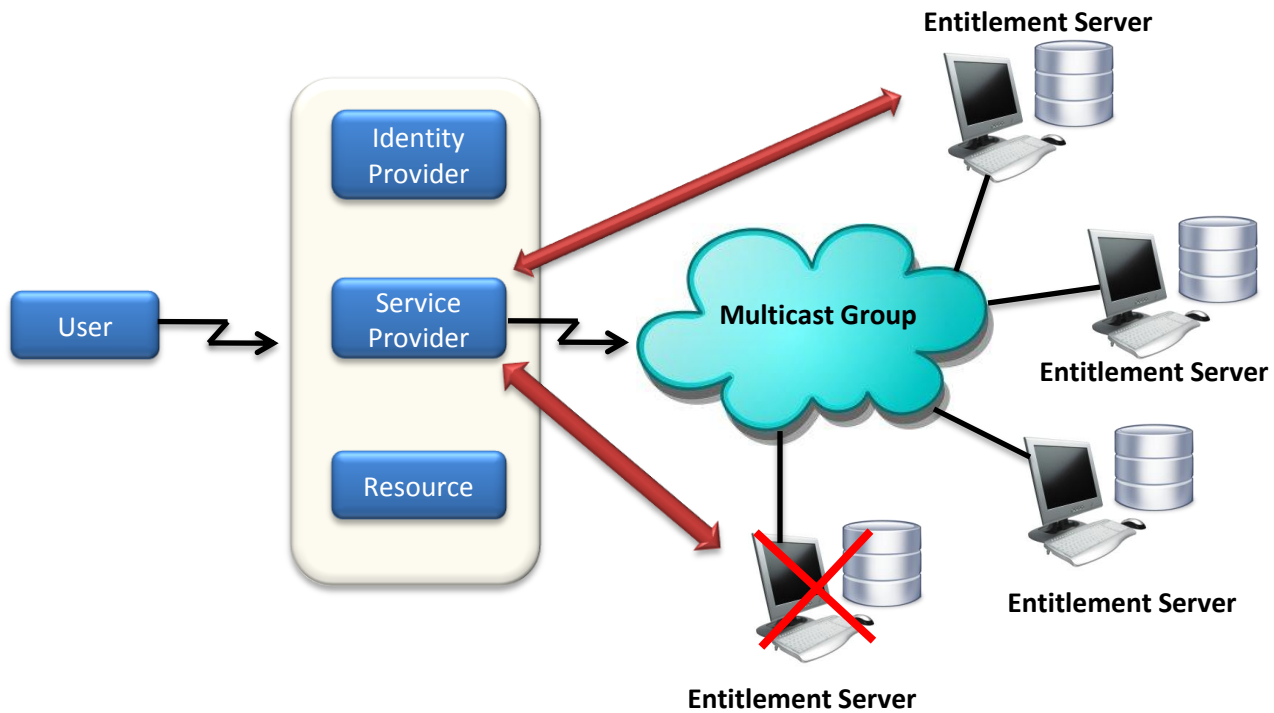
# Issues with Single Entitlement Server

- Service provider needs to know the details where the entitlement server exists
- Failing of the entitlement server causes failure of the authorization process

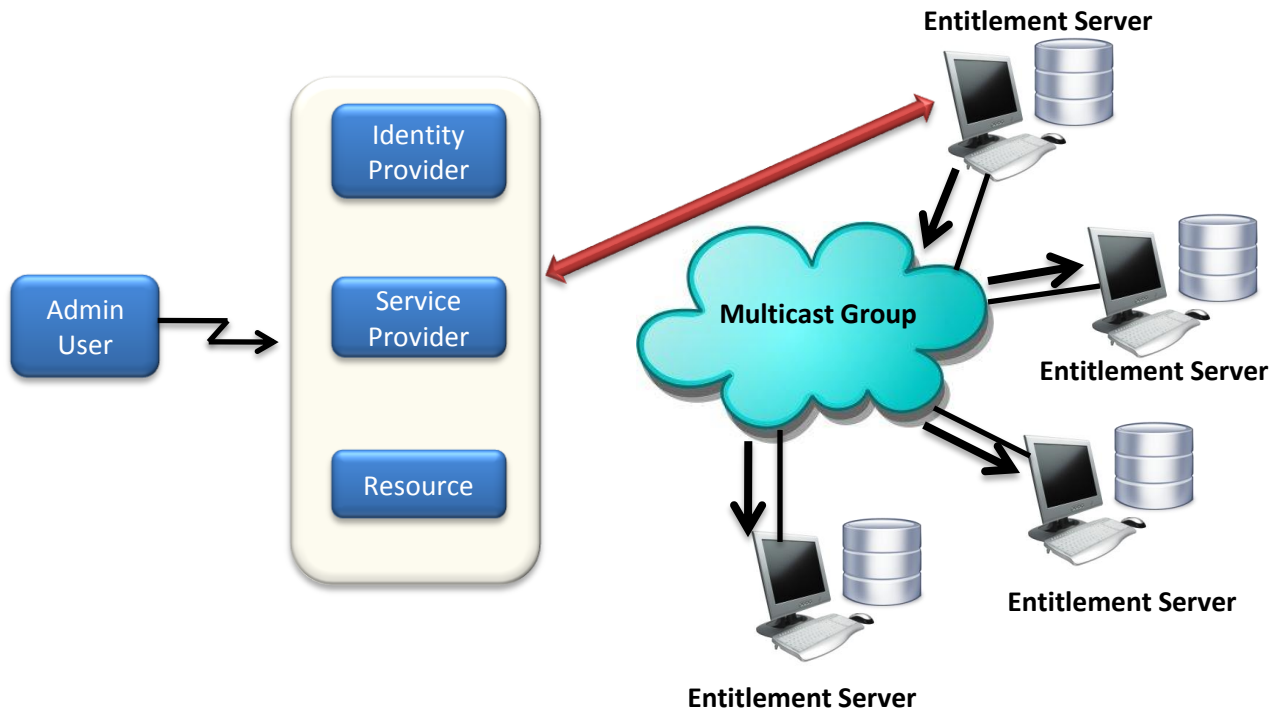
# Strategy

- Multiple entitlement servers
- Multicast Protocol
- All the entitlement servers forms a logical group using multicast network protocol

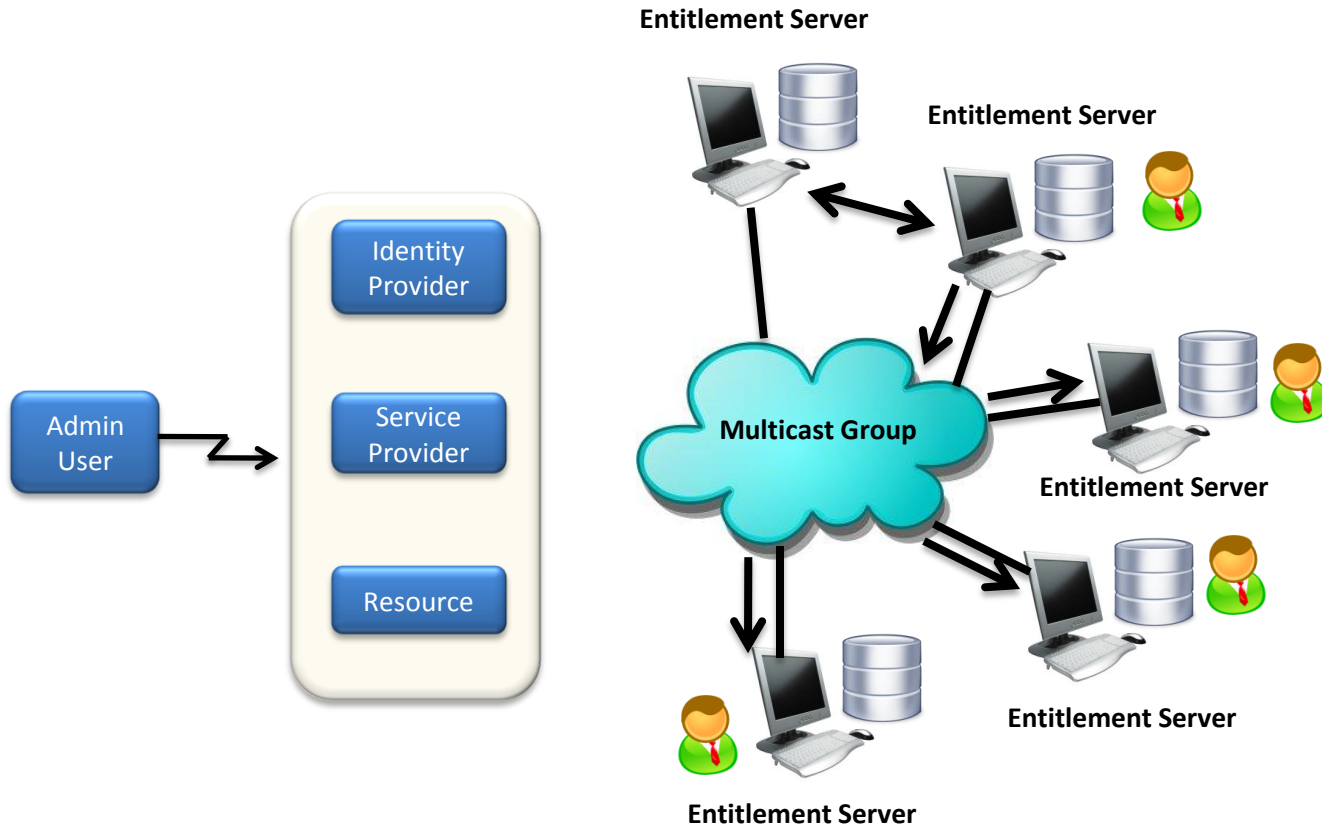
# Process Flow



# Data Consistency



# Data Synchronization



# Conclusion

- Eliminates the failure of authorization process at Virtual Organization level
- Highly Scalable authorization process
- Entitlement server can move from one physical machine to another without affecting process

# References

- <http://shibboleth.internet2.edu/>
- <http://www.internet2.edu/>
- Shibboleth-based Access to and Usage of Grid Resources by R. O. Sinnott, J. Jiang, J. Watt, O. Ajayi September 2006 GRID '06: Proceedings of the 7th IEEE/ACM International Conference on Grid Computing Publisher: IEEE Computer Society
- *“Federated Security: The shibboleth Approach”* by R.L. “Bob” Morgan, Scott Cantor, Steven Carmody, Walter Hoehn and Ken Klingenstein. November 2004 EDUCAUSE QUARTERLY
- Makofske and Almeroth *“Multicast Sockets: Practical Guide for Programmers”* Morgan Kaufmann Publishers
- Ionut Ovidiu Ciordas, MS (2007). *“Fine-Grained Authorization in the Great Plains Network Virtual Organization”* Master’s Thesis. University of Missouri – Columbia: USA.

# Initial Authorization Check

GP.Middleware Shibboleth VO MCast- Access - Mozilla Firefox



File Edit View History Bookmarks Tools Help

http://web.rnet.missouri.edu/GPN-Test/

GN CMN Dictionary Facebook Gmail Google Mizzou Mizzou CS myZou Orkut PunSongs The Times of India Webmail YouTube

GP.Middleware Shibboleth VO MC...

Entitlement Checks ...  
SPPincipal=web.rnet.missouri.edu@missouri.edu  
user=singh@missouri.edu  
SPVO=greatplains.net  
user VO=greatplains.net  
Needed entitlement: urn:mace:greatplains.net:GPNVO  
Perform SP Lookup 2  
b[0] = NO SERVER INFO FOUND  
b[1] = SP\_SETUP\_REQUIRED  
**Perform SP SETUP**  
a[0] = SP\_AUTHENTICATION\_SUCCESS  
a[1] = SP\_SETUP\_SUCCESS  
**Trying SP Lookup again**  
c[0] = SP\_SESSION\_OK  
c[1] = USER\_ENTITLEMENT\_LOOKUP\_SUCCEEDED  
c[2] = Entitlement check done with Server [128.206.116.112]

 **GP.Middleware Shibboleth VO MCast**   
**Access**

---

Access to Site Data  
Project Access

# Further Authorization takes place with same ES

The screenshot shows a Mozilla Firefox browser window with the following details:

- Browser Title:** GP.Middleware Shibboleth VO MCast - Access - Mozilla Firefox
- Address Bar:** http://web.rnet.missouri.edu/GPN-Test/
- Navigation Bar:** Includes icons for CNN, Dictionary, Facebook, Gmail, Google, Mizzou, Mizzou CS, myZou, Orkut, PunSongs, The Times of India, Webmail, and YouTube.
- Page Content:**
  - Entitlement Checks ...
  - SPPrincipal=web.rnet.missouri.edu@missouri.edu
  - user=singh@missouri.edu
  - SPVO=greatplains.net
  - user VO=greatplains.net
  - Needed entitlement: urn:mace:greatplains.net:GPNVO
  - Perform SP Lookup 2
  - b[0]= SP\_SESSION\_OK
  - b[1]= USER\_ENTITLEMENT\_LOOKUP\_SUCCEED
  - b[2]= Entitlement check done with Server [128.206.116.112]
- Logos:** GPN logo (left) and Missouri University of Science and Technology logo (right).
- Text:** GP.Middleware Shibboleth VO MCast Access
- Decorative Elements:** A horizontal bar with blue, green, and red segments.
- Buttons:** Access to Site Data (green text) and Project Access (button).

# Renewing of Secure Channel

GP.Middleware Shibboleth VO MCast - Access - Mozilla Firefox



File Edit View History Bookmarks Tools Help

http://web.rnet.missouri.edu/GPN-Test/

CNN Dictionary Facebook Gmail Google Mizzou Mizzou CS myZou Orkut PunSongs The Times of India Webmail YouTube

GP.Middleware Shibboleth VO MC...

Entitlement Checks ...  
SPPrincipal=web.rnet.missouri.edu@missouri.edu  
user=singh@missouri.edu  
SPVO=greatplains.net  
user VO=greatplains.net  
Needed entitlement: urn:mace:greatplains.net:GPNVO  
Perform SP Lookup 2  
b[0]= SP\_AUTHENTICATION\_SUCCESS  
b[1]= USER\_ENTITLEMENT\_LOOKUP\_SUCCEED  
b[2]= Entitlement check done with Server [128.206.116.112]

 **GP.Middleware Shibboleth VO MCast**   
**Access**

---

Access to Site Data  
Project Access

# Authorization with new ES as previous does not exist in network

GP.Middleware Shibboleth VO MCast - Access - Mozilla Firefox



File Edit View History Bookmarks Tools Help

http://web.rnet.missouri.edu/GPN-Test/

CNN Dictionary Facebook Gmail Google Mizzou Mizzou CS myZou Orkut PunSongs The Times of India Webmail YouTube

GP.Middleware Shibboleth VO MC...



Entitlement Checks ...  
SPPrincipal=web.rnet.missouri.edu@missouri.edu  
user=singh@missouri.edu  
SPVO=greatplains.net  
user VO=greatplains.net  
Needed entitlement: urn:mace:greatplains.net:GPNVO  
Perform SP Lookup 2  
b[0] = ES\_DID\_NOT\_RESPOND  
b[1] = SP\_AUTHENTICATION\_SUCCESS  
b[2] = SP\_SESSION\_OK  
b[3] = USER\_ENTITLEMENT\_LOOKUP\_SUCCEED  
b[4] = Entitlement check done with Server [128.206.116.66]

 **GP.Middleware Shibboleth VO MCast Access** 

---

Access to Site Data  
Project Access

# Administrator Option




 **GP.Middleware Shibboleth VO MCast**   
**Access**




---




**Access to Site Data**

---

**Participants**



[Presentations](#)

5/26/2010

# Identifying self Privilege and Virtual Organization

GP.Middleware Shibboleth VO- Entitlement Management - Mozilla Firefox

https://web.rnet.missouri.edu/GPN-Test/authtest/

 **GP.Middleware Shibboleth VO Entitlement Management** 

Please select a role:

Administrator     Root Administrator

Virtual Organization:

[Print This Page](#)

Page Generated Mon May 31 14:34:26 2010  
Please send comments to: [wwwadm@rnet.missouri.edu](mailto:wwwadm@rnet.missouri.edu)

# Entitlement Management

b[0] = SP\_SESSION\_OK  
b[1] = USER\_ENTITLEMENT\_LOOKUP\_SUCCEED  
b[2] = Entitlement check done with Server [128.206.116.66]



## GP.Middleware Shibboleth VO Mcast Entitlement Management



Please use the following options in order to accomplish your task.

Your privilege level: **root**

Your virtual organization: **greatplains.net**

Please select one and fill the text boxes below accordingly:

- Add a new entitlement - Fill *User Name, Institution Name, Virtual Organization Name, Entitlement value*
- Delete an existing entitlement - Fill *User Name, Institution Name, Virtual Organization Name, Entitlement value*
- Lookup an existing entitlement - Fill *User Name, Institution Name, Virtual Organization Name, Entitlement value*
- Display all entitlements of the user - Fill *User Name, Institution Name, Virtual Organization Name value*
- Display all the users with the entitlement - Fill *Entitlement value*
- Display all records
- Logout

User Name:

Institution Name:

Virtual Organization:

Entitlement value:



The values "user", "admin" or "root" are reserved. Please use only if appropriate!

# Improper Entitlement

GP.Middleware Shibboleth VO Mcast - Entitlement Management - Mozilla Firefox

https://web.met.missouri.edu/GPN-Test/authtest/process.php

```
DebugProcess: debug=2
DebugProcess: UEntitle=GPNVO
eppn = singh@missouri.edu
SPUserName: web.met.missouri.edu
lookup: privilege=admin
db_client 20 web.met.missouri.edu@missouri.edu greatplains.net singh@missouri.edu greatplains.net admin
b[0]= SP_AUTHENTICATION_SUCCESS
b[1]= USER_ENTITLEMENT_LOOKUP_FAILED
b[2]= Entitlement check done with Server [128.206.116.112]
```

 **GP.Middleware Shibboleth VO Mcast**   
**Entitlement Management**

---

**Unauthorized access: You do not have proper entitlement to access page**

# No ES present in the network

GP.Middleware Shibboleth VO Mcast - Entitlement Management - Mozilla Firefox

https://web.rnet.missouri.edu/GPN-Test/authtest/process.php

DebugProcess: debug=2  
DebugProcess: UEntitle=GPNVO  
eppn = singh@missouri.edu  
SPUserName: web.rnet.missouri.edu  
lookup: privilege=admin  
db\_client 20 web.rnet.missouri.edu@missouri.edu greatplains.net singh@missouri.edu greatplains.net admin  
b[0] = NO\_SYM\_KEY\_FOUND  
b[1] = ES\_DID\_NOT\_RESPOND  
b[2] = ES\_DID\_NOT\_RESPOND  
b[3] = ES\_DID\_NOT\_RESPOND  
b[4] = SP\_SETUP\_REQUIRED  
NO ES RESPONDED  
PERFORM SP\_SETUP  
a[0] = NO\_SERVER\_RESPONDED

 **GP.Middleware Shibboleth VO Mcast  
Entitlement Management** 

---

**Unauthorized access: Please contact Administrator**

Thanks  
&  
Questions ?