



Duke Systems

CF AUTHN/AUTHZ
GEC10

Jeff Chase
Duke University



GENI Security Architecture

- **IMHO, security is a major recurring problem in GENI Control Framework (CF) architecture.**
- **The problem comes when we attempt to anchor/connect GENI to the outside world.**
 - **Confusion about trust roots**
 - **Ad hoc identity silos, etc.**
 - **Federation → federated identity**
- **Solution: factor out security architecture.**
 - **Do it once.**
 - **Do it right.**

Principles

- **Design in federation from the ground up.**
- **Separate policy from mechanism.**
- **Play well with others.**
- **Use off-the-shelf solutions when suitable.**
 - **External identity providers (IdPs)**
 - **“Web of identities”**
 - **Attribute-based access control (ABAC)**
 - **“Web of roles”**
 - **[See my GEC7 and GEC8 presentations.]**

GENI Security Architecture

- **Agreement on underlying mechanisms:**
 - **Endorsement of identity**
 - **Assertion of attributes**
 - **Delegation of rights**
 - **Anchored in some set of trust roots**

Issued by whom? How are the subjects named?

What are the attributes, rights, etc.? How to broker trust?

How are authorization policies specified?

Bank
password:
goMets12

e-mail:
letmein

credit card:
bowser8

brokerage:
initial23

Log in

https://login.postini.c

Google

Log in to your message center.

Invalid log in or server error. Please try again.

[Forgot your password?](#)

Log in Address
example: joe234@jumbowidgetsco.com

Password
note: password is case-sensitive

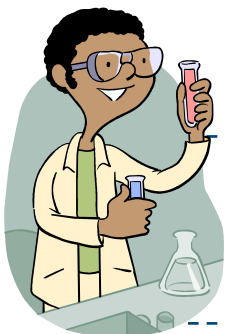
Remember my Address and Password ([what is this?](#))

Done login.postini.com

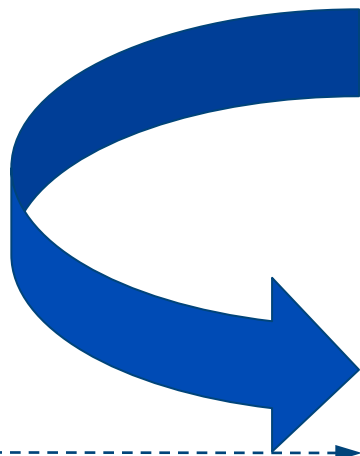
External Identity Providers in GENI (?)

- **GENI should enable/permit external IdPs.**
 - Leverage powerful identity solutions developed by the large community focused on that problem.
 - Free GENI participants from administering identities and accounts.
- **Which IdPs? Shibboleth and perhaps others.**
 - Shibboleth is mature and widely deployed by universities and other institutions.
 - Single Sign On (SSO)

Authenticated user identity
Attributes for authorization



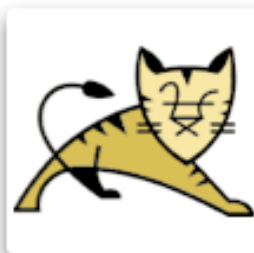
User/experimenters
and “hands-free”
tools



HTTPS
XMLRPC / SOAP



Duke Shibboleth
Identity Provider (IdP)



Web Service Portal
(SP)

Anonymous User

Login



home

About

Contact Us

About this Site

- » NSF GENI
- » GENI-ORCA Project
- » Duke NICL Lab
- » Apache Jakarta
- » Velocity

NetID Services

duke.edu https://shib.oit.duke.edu/idp/Authn/Us

Most Visited Getting Started Latest Headlines

NetID Services instructions - GENI... Perspectives Gec8ClusterDAgen...



Duke University NetID Services

Please identify yourself to NetID service handleservice at host shibboleth.duke.edu.

Please enter your NetID and password:

NetID:

Password:

Don't know what a NetID is? Not sure if you have one? [Find out.](#)

Forgot your password? [Click here.](#)

[GEC8 ORCA/Shib demo slides]

Orca Web Portal 2.0

http://pod1.cod.cs.duke.edu:8080/orca/secure/secure.vm

Google

Most Visited ▾ Getting Started Latest Headlines ↗

Orca Web Portal 2.0 instructions - GENI-O... Perspectives Gec8ClusterDAgenda ...

Jeff Chase Logout



home user broker site admin About Contact Us

About this Site

- » NSF GENI
- » GENI-ORCA Project
- » Duke NICL Lab
- » Apache Jakarta
- » Velocity

Hello Jeff Chase. Welcome to Orca Portal.

Login Id: chase@duke.edu

Name Id: _55710762d32db7e276501ebfcc68ad06

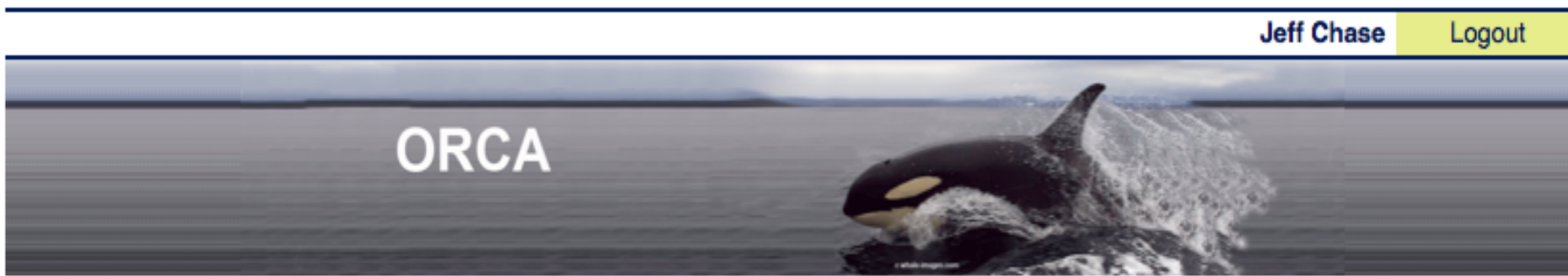
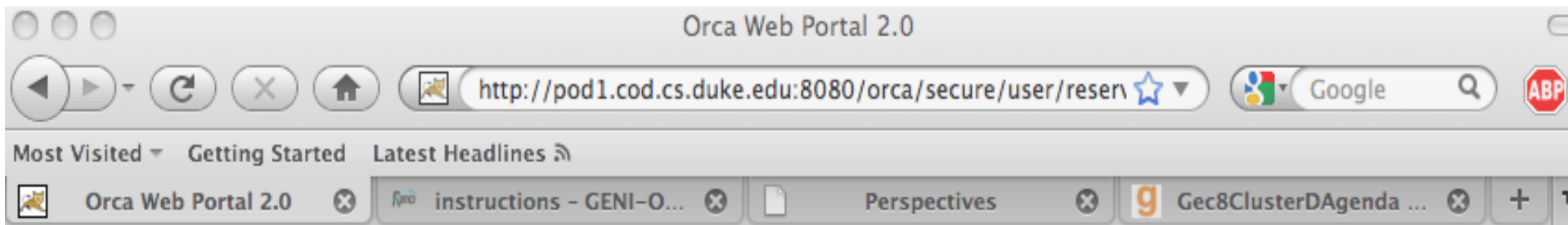
You are a member of the following groups.

- urn:mace:duke.edu:groups:cs:geni:test

Shibboleth Attributes:

- urn:oid:1.3.6.1.4.1.5923.1.5.1.1 (isMemberOf): [urn:mace:duke.edu:groups:cs:geni:test]
- urn:oid:1.3.6.1.4.1.5923.1.1.1.6 (eduPersonPrincipalName): [chase@duke.edu]
- urn:oid:1.3.6.1.4.1.5923.1.1.1.9 (eduPersonScopedAffiliation): [faculty@duke.edu]

[GEC8 ORCA/Shib demo slides]



- home
- user**
- broker
- site
- admin
- About
- Contact Us

- Slices**
 - » View Slices
 - » Create Slice
- Reservations**
 - » Create Reservation
 - » View All Reservations
- Slice Controllers**
 - » View Controllers
 - » Start Controller
- My Account**
 - » Current Actor
 - » Actors
 - » Settings

Create Reservation

Broker	<input type="text" value="broker"/>	Resource Attributes
Resource Pool	<input type="text" value="Virtual Machine"/>	Memory 128MB
Units *	<input type="text" value="5"/>	CPU 1/2 of 2GHz Intel Xeon
Lease Start *	<input type="text" value="07/16/2010 16:29"/>	
Lease End *	<input type="text" value="07/17/2010 16:29"/>	
	<input type="button" value="Create"/>	<input type="button" value="Cancel"/>

[GEC8 ORCA/Shib demo slides]



Jeff Chase Logout

- Slices**
 - » View Slices
 - » Create Slice
- Reservations**
 - » Create Reservation
 - » View All Reservations
- Slice Controllers**
 - » View Controllers
 - » Start Controller
- My Account**
 - » Current Actor
 - » Actors
 - » Settings

Reservations

Select: All None Action:

No	Slice	Type	Units [R]	Units [A]	Start	End	Broker	Site	State
<input type="checkbox"/>	1	service	Virtual Machine	5	5	07/17/2010 15:48	07/18/2010 15:48	broker	Failed manage

Select: All None Action:

[GEC8 ORCA/Shib demo slides]

Reservation Details

Actions	<input type="button" value="Close"/> <input type="button" value="Remove"/>
Reservation ID	92fcd943-7675-458a-af0b-5e3480a9d6bb
Resource Type	Virtual Machine
Requested Units	5
Assigned Units	5
Leased Units	0
Lease Start	07/17/2010 15:48
Lease End	07/18/2010 15:48
Broker	broker
Site	
State	Failed
Status Message	You are authorized to reserve a maximum of 2 units.
Units	No units.

Allocation policy considers group membership attributes of requester (ABAC).

My enrollment

[My memberships](#)

[Join groups](#)

My responsibilities

Manage groups

[Create groups](#)

My tools

[Explore](#)

[Search](#)

[Folder workspace](#)

[Group workspace](#)

[Entity workspace](#)

[Help](#)

Grouper is sponsored by



Manage groups

To find groups where you may update the membership lists, or assign privileges, you can:

- Browse the groups hierarchy
- List your groups
- Search for groups by name

Browse or list groups [List my groups](#)

Current location is:

 Duke University:  Computer Science:  **GENI**

Showing 1-1 of 1 items

Click a folder name to view its direct members, or a group name to see its summary

 test

Search groups [Advanced groups search](#)

[Search groups](#)

Search from

Display results by Path Name ID Path

Manage folders

Current location is:

 Duke University:  Computer Science:  **GENI**

[Add to Folder workspace](#) [Create group](#) [Moves and Copies](#) [Audit log](#)

[GEC8 ORCA/Shib demo slides]

Attribute-Based Access Control (ABAC)

- **This simple example illustrates Shib + ABAC.**
- **The attributes are asserted by a Shib IdP.**
- **The resource allocation policy trusts and understands attributes from this source.**
- **The policy uses the attributes to make a policy decision.**
 - **Authorization**
 - **Resource Control**
- **Shibboleth and ABAC work together.**

Shibboleth in GENI, IMHO

- **Easy to use to authenticate user/browser at a portal “at the edge”.**
- **Once authenticated, user can upload a public key for use by “hands-free” tools.**
 - **Standard for existing testbeds and clouds**
 - **Leverages external IdPs and avoids PKI**
- **Continue to use GENI key-based mechanisms internally.**
- **Continue to explore potential of delegated authentication, but do not depend on it.**

GENI Portal (GIdP)

- **GENI identity portal (GIdP) is any web app that authenticates users and issues GENI certs.**
 - **Acts as a trust anchor:** other GENI CF actors must trust the portal to do it right (act as a CA).
 - **Bridges GENI to external IdPs** (e.g., Shib) and/or has built-in account manager (e.g., PG&L).
 - **Helps find “one throat to choke”:** if a user misbehaves, its GIdP can hold it accountable.
 - **Interfaces to institutional IT services for users.**

Implementation: CF View

- **Factors authn and CH user registry OUT of the control framework.**
 - So: “no implementation required.”
- 1. **Register trust anchors in each CF actor.**
- 2. **Install authz policies to consider attributes (e.g., using ABAC).**
- 3. **May need to pass certs through...**
- 4. **Allow for revocation...**



Duke Systems

CF AUTHN/AUTHZ
GEC10

Jeff Chase
Duke University



GENI Security Architecture

- **IMHO, security is a major recurring problem in GENI Control Framework (CF) architecture.**
- **The problem comes when we attempt to anchor/connect GENI to the outside world.**
 - **Confusion about trust roots**
 - **Ad hoc identity silos, etc.**
 - **Federation → federated identity**
- **Solution: factor out security architecture.**
 - **Do it once.**
 - **Do it right.**

Principles

- **Design in federation from the ground up.**
- **Separate policy from mechanism.**
- **Play well with others.**
- **Use off-the-shelf solutions when suitable.**
 - **External identity providers (IdPs)**
 - **“Web of identities”**
 - **Attribute-based access control (ABAC)**
 - **“Web of roles”**
 - **[See my GEC7 and GEC8 presentations.]**

GENI Security Architecture

- **Agreement on underlying mechanisms:**
 - **Endorsement of identity**
 - **Assertion of attributes**
 - **Delegation of rights**
 - **Anchored in some set of trust roots**

Issued by whom? How are the subjects named?

What are the attributes, rights, etc.? How to broker trust?

How are authorization policies specified?

Trust Anchors

- **Key question for CF architecture: what are the trust anchors/roots for the trust fabric?**
 - SA, MA, CH, ...etc.
- **Part of the beauty of ABAC is that any entity may serve as a trust anchor for its own name space of attributes.**
 - Of course...authz PDP must choose to accept those attributes.

Point 1. External IdPs and ABAC go together: IdPs serve as attribute sources for ABAC policies.

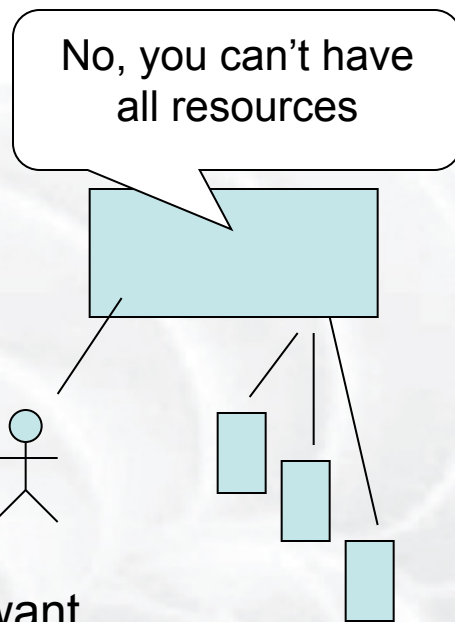
IdPs as Trust Anchors

- **An IdP (e.g., Shib) is just a trust anchor maintained by an institution.**
- **The IdP authenticates the user agent (login).**
- **IdP asserts attributes of the user identity.**
 - **E.g., signed assertion of attributes of identity bound to an HTTPS session.**
 - **E.g., “Duke CS grad student”.**
- **Authorization policy in the server can consider these attributes (e.g., ABAC).**
 - **“Duke students may use this facility on Monday.”**

Point 2. Resource allocation is not (just) an authorization problem.

Enforcing system-wide policy as needed

Implement system-wide policy as needed.



“I want them all!”

Identified Aggregates

Enable system-wide usage policies as the need arises.

“The GENI system shall provide mechanisms to implement clearinghouse-wide resource allocation policies.... This will allow funding agencies or other component contributors to put overall constraints on how their components will be used.”



Reservation Details

Actions	<input type="button" value="Close"/> <input type="button" value="Remove"/>
Reservation ID	92fcd943-7675-458a-af0b-5e3480a9d6bb
Resource Type	Virtual Machine
Requested Units	5
Assigned Units	5
Leased Units	0
Lease Start	07/17/2010 15:48
Lease End	07/18/2010 15:48
Broker	broker
Site	
State	Failed
Status Message	You are authorized to reserve a maximum of 2 units.
Units	No units.

Allocation policy considers group membership attributes of requester (ABAC).

Resources: The ORCA View

- **ORCA has pluggable resource allocation policy in AMs and brokering services.**
- **These policies may consider ABAC attributes.**
- **They may need other information as well:**
 - **Resource status**
 - **Allocation history of this client, group, or slice**
 - **Allocations and promises to other slices**
 - **Payment by (virtual) currency?**
 - **Resource delegation directives (**tickets**).**
- **ABAC is helps but is not sufficient.**

Point 3. There are many other (potential) attribute roots other than IdPs.

Slice owners as attribute roots

- **Would an AM trust a “random” user/ experimenter as a credential source?**
- **Yes, to delegate control privileges for the objects they create.**
- **E.g., slice owner to empower others to operate on a slice.**
- **ABAC delegation primitives are sufficiently powerful to do this.**

SFA 2.0, Section 8

“A capability system is a special case of an ABAC framework in which all attributes directly represent specific privileges for specific objects. This restriction offers a significant simplification: since a credential represents directly the privileges that it enables, any entity may determine those privileges by inspecting that credential alone: **no inference procedure is required.**”

But...

- **For GENI, ABAC needs a limited form of parameterized roles/attributes.**
- **Ownership attributes are rooted in the object creator (or the SA), not in the AMs.**
- **That requires some parameterization of the authz policy for objects on creation.**
- **We can replace the SFA registered capability authz model in a straightforward way.**

Point 4. ABAC can support other features we need in the GENI trust fabric.

Example: “Stop the Experiment!”

- **Add local attributes to objects.**
 - “A slice endorsed by a GENI-affiliated SA is a GENI slice.”
- **Add local object attributes to the ABAC inference engine.**
 - “If S is a GENI slice, then any entity with the GMOC role may suspend S.”



Example: User Delegation of Authority

- **SpeaksFor** attribute for automated controllers.
 - “Designated driver”
- **E.g., “This controller speaks for me with respect to operations on slice S.”**
 - This server can act as an owner of S.
 - But I am responsible for what it does.

Other?

- **Cyberphysical systems?**
 - “Don’t point the camera at the sun?”
- **OpenFlow control of flowspace?**
- **Experiment opt-in?**

Conclusion

- **I support this proposal.**
- **Credential format needs some work.**
- **We need to standardize conventions for the basic attributes and their flow.**
 - e.g., for user-created objects
- **ABAC may need “just a few tweaks”.**
- **Eschew credential negotiation.**

eom

ABAC Credential Types

1. $A.r \leftarrow D$

A says that D has the role A.r.

2. $A.r \leftarrow B.r1$

A says that any member of the role B.r1 is also a member of A.r.

3. $A.r \leftarrow A.r1.r2$

"If someone who A says has the attribute r1 then says somebody has the attribute r2, then A says that somebody has the attribute A.r." "This is an attribute-based delegation

Implicit type three rule: $A.r \leftarrow A.r.r$

(delegation of identity attribute is a special case: speaks for ...not transitive)

4. intersection

$A.r \leftarrow$ (intersection of a bunch of other roles)