

# eXtreme Scale Identity Management for Scientific Collaborations (XSIM)

---

*Bob Cowles, Craig Jackson, Von Welch*

*Identity Management Collaboration Meeting  
Chicago, IL  
August 28<sup>th</sup>, 2013*



**CENTER FOR APPLIED  
CYBERSECURITY RESEARCH**

---

INDIANA UNIVERSITY  
Pervasive Technology Institute

# The VO's impact on IdM

The VO has proven itself as the key way of allowing large-scale science collaborations.

However, there is great variance in how IdM for VOs is implemented.



CENTER FOR APPLIED  
CYBERSECURITY RESEARCH

INDIANA UNIVERSITY  
Pervasive Technology Institute

---

## **XSIM Goal**

Understand how IdM has been deployed to support VOs over the past 15 years.

Glide-ins, science gateways, community accounts, etc.

Understand why we did what we did.

Organize that information to guide us into the future.



---

# XSIM Approach

Analyze implementations – semi-structured interviews and literature study of the different VO IdM approaches.

Discern and describe the different relationships between VOs and their resource providers.

Derive a model for an evolutionary step in IdM that describes trust relationships between collaborations, resource providers and users, and when different relationships make sense.



---

# Model Basis: VO IdM Lifecycle

- Enrollment
- Provisioning
- Request
- Usage
- Incident Management
- De-provisioning

Each lifecycle stage has a small number of possible VO/RP interactions.

First exposure of user-specific information is a big one.



TABLE II. INTERVIEW RESULTS CAST INTO OUR VIRTUAL ORGANIZATION IDENTITY MANAGEMENT MODEL

Context			VO IdM Model Parameters					
<i>Relationship</i>	<i>Resource</i>	<i>Type of Access</i>	<i>When is IdM information provided to RP?</i>	<i>Enrollment</i>	<i>Provisioning</i>	<i>Request</i>	<i>Usage</i>	<i>Incident Handling</i>
ATLAS & Brookhaven	Batch	Arbitrary exec	IR	VO	Group	VO	VO Group	RP
ATLAS & Brookhaven	Wiki	Web	Provisioning	VO	User	User	Known Isolated	RP
ATLAS & Brookhaven	CVS	Shell	Provisioning	VO	User	User	Known Isolated	RP
ATLAS & AGLT2	Batch	Arbitrary exec	IR	VO	Group	VO	VO Group	From VO
various & Brookhaven	Batch	Arbitrary exec	Never	VO	Group	VO	VO Group	Blacklist VO
Alice & Brookhaven	Batch	Arbitrary exec	IR	VO	Group	VO	VO Group	VO
CMS Fermilab &	Batch	Arbitrary exec	Request	VO	Pool	VO	VO Isolated	RP
CMS Fermilab &	News	Web	Request	VO	User	User	Known Isolated	RP

...for 14 different VO-RP relationships.



---

## Future work

- Apply the model in practice and evolve it from descriptive to providing guidance.
- Fully understand the trust implications of the model.
- Examine different types of RPs – commercial clouds, HPC – to stretch model.



---

# Thank you

Robert Cowles, Craig Jackson and Von Welch. *Identity Management for Virtual Organizations: A Survey of Implementations and Model*. eScience 2013 (to appear), 2013.

<http://cacr.iu.edu/collab-idm>

We thank the Department of Energy Next-Generation Networks for Science (NGNS) program (Grant No. DE-FG02-12ER26111) for funding this effort.

The views and conclusions contained herein are those of the author and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the sponsors or any organization.

