# XSIM

Extreme Scale Identity Management

# Facilitating Scientific Collaborations by Delegating Identity Management

Von Welch (PI), Bob Cowles, Craig Jackson

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

June 15, 2015

Second Workshop on the Changing Landscape in HPC Security

# The XSIM Team

- **Von Welch** – CACR Director, long time distributed science security researcher.
- **Bob Cowles** – BrightLite Information Security, former CISO of SLAC.
- **Craig Jackson** – CACR Senior Policy Analyst, recovering litigator.

# IdM is Critical for Enabling Science

- Access to instruments and data
- Embodying the membership and structure of the VO
- Ensuring credit / names on papers

# Virtual Organization IdM

We have 15 years+ of applied experimentation in virtual organization (VO) IdM.

A number of approaches have been tried:

VOMS, Glide-ins, Science gateways, COManage, Community/group accounts

# XSIM’s Goals

1. Develop a descriptive VO-IdM model that expresses observed variations in collaboratory identity architectures…

   ...in a way that scientists/Craig can understand.

2. Understand the reasons for and factors influencing those observed variations.

3. Leverage that model into guidance for structuring new VO-RP relationships and evolving existing ones.

# Our Process

# Semi-Structured Interviews with ~20 VOs and RPs

Collaboratories

- Atlas
- BaBar
- Belle-II
- CMS
- Darkside
- Engage
- Earth System Grid
- Fermi Space Telescope
- LIGO
- LSST/DESC

Resource Providers

- Atlas Great Lakes T2
- FermiGrid
- GRIF
- U. Nebraska (CMS)
- LCLS
- RAL
- GRIF/LAL
- LLNL
- NERSC
- Blue Waters

# We were like….

- What did you do?
- What did you want to do?
- Why did you do what you did?

# Our Model

# *Some core findings….*

1. The VO can and often does play a role in collaboratory IdM implementation.
2. This VO role alters the traditional direct trust relationship between users and RPs.
3. We've seen a variety of different approaches at this RP-to-VO *delegation* of IdM tasks.
4. Trends are toward *mediated trust*, utilizing the VO's capacity to represent its members.

# VO IdM Model: *Data-centric needed to describe all this variation.*

Identity data is ***produced*** to enable workflows.

Identity data is ***consumed*** to perform IdM functions.

## Types of Identity Data

1. User “identity”
2. User contact info
3. VO membership / role

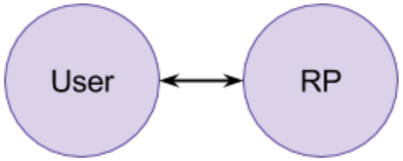
## IdM Functionalities

A. authentication
B. authorization
C. allocation/scheduling
D. accounting
E. auditing
F. user support
G. incident response

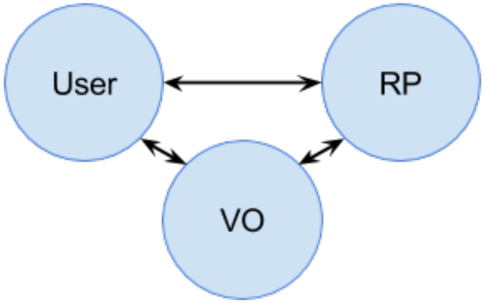
# VO IdM Trust Model Extremes

… via 800-39

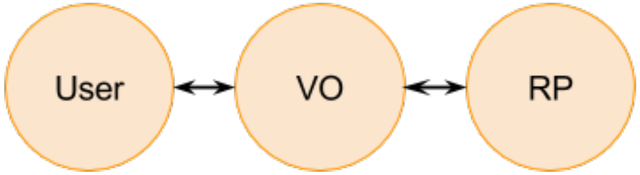
***Classically*** RPs produced and consumed all IdM data.



***Brokered trust relationships*** entail VOs & TTPs generating user data, to be consumed by RPs.

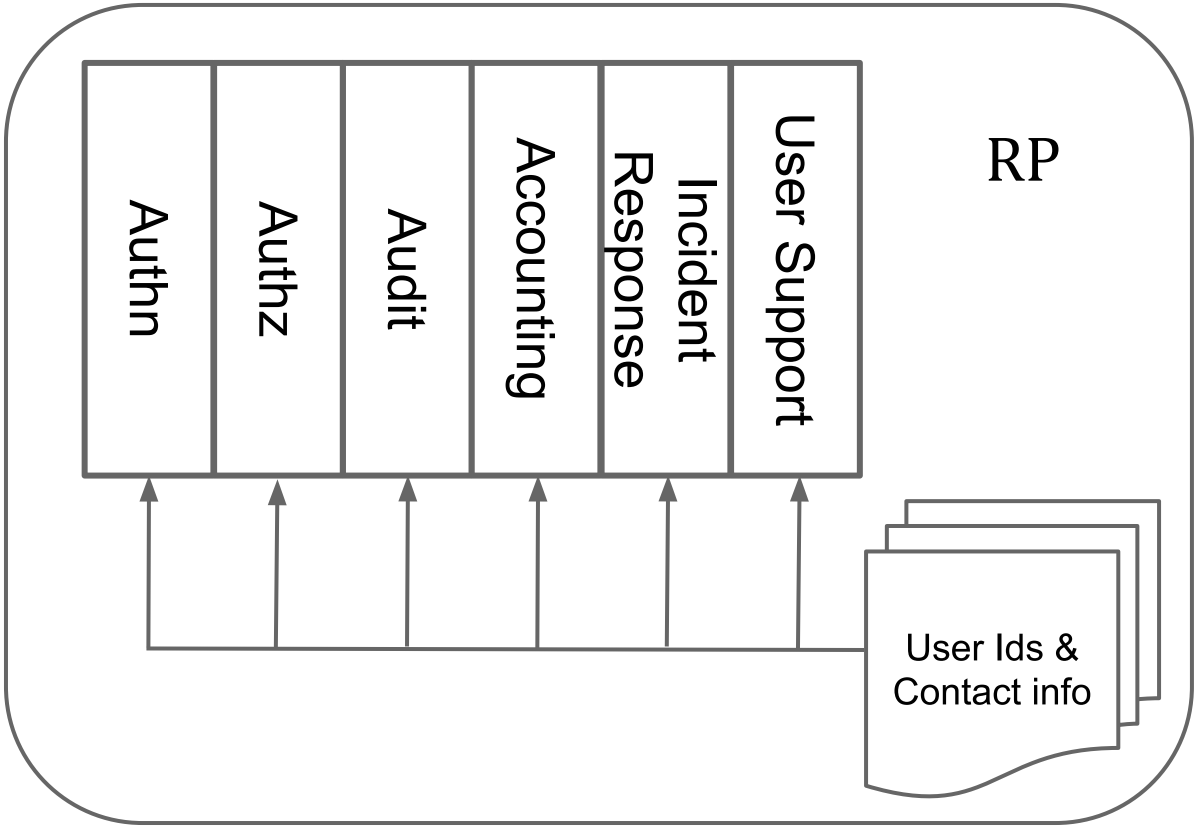


***Transitive trust relationships*** forego all user data consumption by RP.

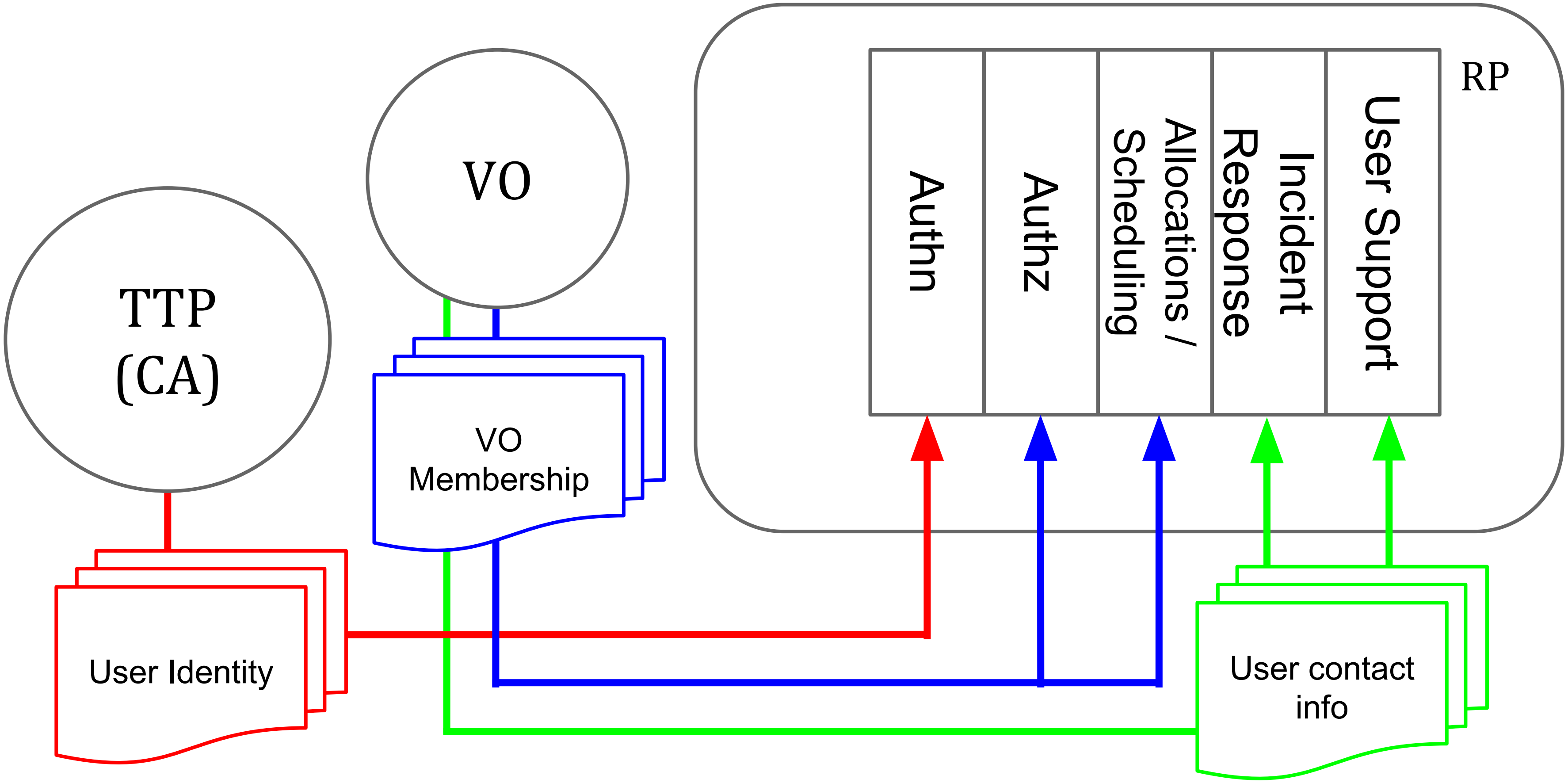


# Identity Data Flow in the "Classic Model"

RP produces and consumes all IdM information.



# Identity Data Flow in Multi-user Pilot Jobs Brokered Trust



# Goal 1: ACHIEVED

1. ~~Develop a descriptive VO IdM model that expresses observed variations in collaboratory identity architectures….~~

   ~~…in a way that scientists/Craig can understand.~~

Why this shift toward more delegation?

Why isn’t everybody going there?

What enabled delegation where there was resistance?

# Drivers and Benefits of Sharing IdM

- Allows scaling to more scientists.
- Centralized management of VO policies.
- Places effort where most appropriate.
- Avoid unneeded duplication of IdM data.
- Eases collaboration inside of and across VOs.
- Improves ease of use through better integration with science workflows.
- Efficiency...

# Barriers to Delegating IdM Functions

1. Compliance and Assurance Concerns

2. Risk Aversion / Trust Aversion

3. Historical Inertia *We've always done it this way.*

4. Technology Limitations

# Enablers of Delegation

1. RP-VO existing relationships and explicit agreements

2. User traceability (OSG)

3. Sandboxes (VMs, limited APIs, etc.)

4. *A closer look at the policy and risk environment...*

# Goals 2 and 3:

2. Understand the reasons for and factors influencing those observed variations.

*Pretty good handle on this….*

3. Leverage that model into guidance for structuring new VO-RP relationships and evolving existing ones.

*Been working on this. Produced guidance targeted at OSG, DESC, DOE Labs.*

# Policy Analysis in the CLHS paper:

A closer reading of DOE policy on **Deemed Export** and **Unclassified Foreign Visits** as presumed reasons for identity data production at RPs (DOE Labs), against the backdrop of DOE's **risk management orientation**.

# Deemed Export

- " … the release of controlled technology to a foreign person … "
- An export license is required, EXCEPT:
    - Research involving public information
    - Fundamental research
    - Suppliers of grid or cloud computing
- Can eliminate requirement for identity proofing (needs legal review)

# Unclassified Foreign Visits

- DOE O 142.3A (2010)
- Policy for access to computing resources responsibility of DOE CIO; no policy exists
- Access to scientific information and commercially available technology is not within scope of the order
- Can eliminate requirement for identity proofing (needs legal review)

# Risk Management

- DOE recognized need to shift to risk-based security with O 205.1B in 2011
  - Cyber programs can be flexible if risks are documented and residual risks accepted
  - Implication… If brokered and transitive trust better enable science *and* significantly reduce costs, with little increase in residual risk, then why not go there?
- But, that means embracing a truly risk-based and mission-enabling approach to cybersecurity.

# Related Work

- Work by I2, Klingenstein, et al.
- NSTIC IDESG Functional Model Group.
- NIST 800-39 (Trust Models).
- Lin, Vullings, and Dalziel. “Trust-based Access Control Model for Virtual Organizations.”

# Thank you

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.