



Identity Management for Virtual Organizations

Bob Cowles, Craig Jackson, Von Welch (PI)

2014 Fall EUGridPMA Meeting, Poznań, Poland

September 9, 2014



**CENTER FOR APPLIED
CYBERSECURITY RESEARCH**

INDIANA UNIVERSITY
Pervasive Technology Institute

XSIM's Work on VO IdM

Our Mission

Develop a VO-IdM model that (a) expresses observed variations in collaboratory identity architectures and (b) can be leveraged into guidance for selection.

FY2013

Semi-structured interviews with 20+ VO-RP relationships



FY2014 XSIM Papers and Documents

Robert Cowles, Craig Jackson and Von Welch. *Identity Management for Virtual Organizations: A Survey of Implementations and Model*. 9th IEEE International Conference on eScience, 2013.

<http://www.vonwelch.com/pubs/VOldM13>

Robert Cowles, Craig Jackson and Von Welch. *Identity management factors for HEP virtual organizations*. 20th International Conference on Computing in High Energy and Nuclear Physics (CHEP2013), 2013. <http://www.vonwelch.com/pubs/CHEP2013>

Robert Cowles, Craig Jackson, Von Welch and Shreyas Cholia. *A Model for Identity Management in Future Scientific Collaboratories*. (DRAFT) International Symposium on Grids and Clouds (ISGC) 2014, 2014. <http://www.vonwelch.com/pubs/XSIMISGC2014>

Von Welch, Robert Cowles, and Craig Jackson. *Identity Management Guidance to OSG Virtual Organizations and Resource Providers*. 2014. OSG Documentation Database. <http://osg-docdb.opensciencegrid.org/cgi-bin/RetrieveFile?docid=1199;filename=XSIM%20OSG%20IdM%20Guidance%20-%20June%202014%20-%20v1.pdf;version=1>

Bob Cowles, Craig Jackson, and Von Welch (PI). *DESC Identity Management: Analysis and Recommendations* (DRAFT) for review by DESC. August, 2014.

(Early DRAFT) Article in monthly OSG Newsletter.



Some core findings....

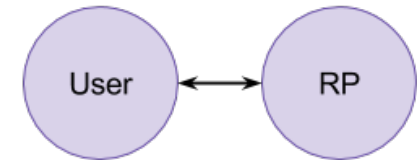
1. The VO can and often does play a role in collaboratory IdM implementation.
2. This VO role alters the traditional direct trust relationship between users and RPs.
3. We've seen a variety of different approaches at this RP-to-VO *delegation* of IdM tasks.
4. Trends are toward *mediated trust*, utilizing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



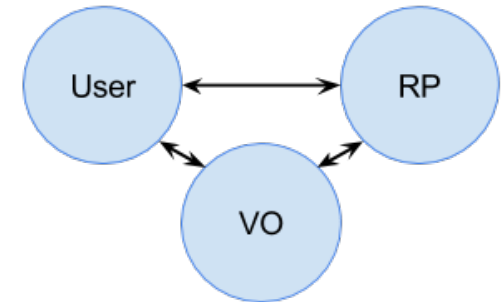
VO IdM Trust Model Extremes

... via 800-39

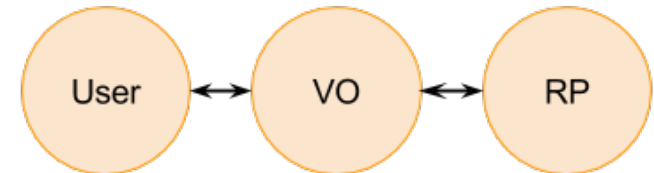
Classically RPs produced and consumed all IdM data.



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



Transitive trust relationships forego all user data consumption by RP.



Pressure -- Simplification

- For users
 - Federated Identity
 - Single signon
- For Resource Providers
 - VO handles Incident Response
 - No individual user interaction
 - Significant savings in Identity Management
- *Portals plus Federated IdM point to a solution*



Types of Factors Affecting Delegation

- **Motivators**
 - These factors drive the delegation of IdM functions due to the perceived benefits
- **Enablers**
 - These factors provide a receptive environment making the delegation of IdM functions easier
- **Barriers**
 - These factors prevent or at least inhibit delegation of IdM functions



Motivators for Delegation

- **Scaling and Dynamicity of VO**
 - RP incurs significant costs to supply IdM for large VOs or VOs with high turnover rates
 - Number of institutions involved is secondary factor -- influences use of 3rd party identity provider
- **Complex VO roles and policies**
 - RP must track and implement access controls
 - Can require greater communication between VO and RP
- **VO-run collaboration services**
 - Wikis or forums isolated to the VO
 - VO-supplied IdM rather than depending on RP
- **VO using multiple RPs**



Enablers of Delegation

- Available VO IT/IdM effort and expertise
 - IT knowledgeable staff to install/maintain servers
 - IdM knowledgeable staff for secure configuration
- Established trust relationships
 - VO has close association with RP or good reputation
 - VO has history or prior collaboration with RP
- Available tracing mechanisms
 - Facilitate user support and incident response
 - Helps mitigate perceived risks from delegation
- Alignment with RP's mission

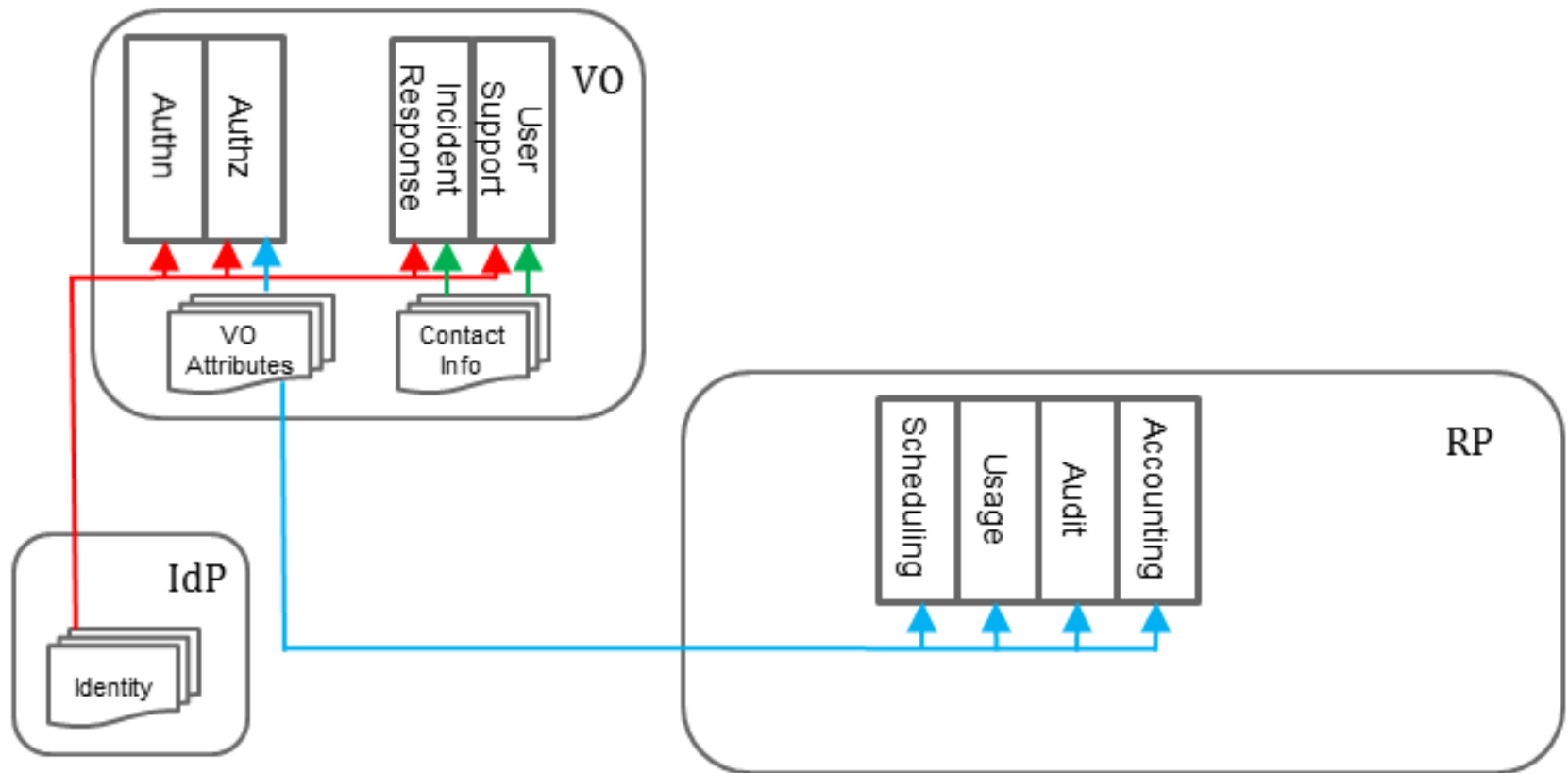


Barriers to Delegation

- Low risk tolerance and historical inertia
 - or “We’ve always done it this way”
 - Changes risk profile
- Compliance and assurance requirements
 - Government regulations or
 - Other oversight or stakeholder requirements
- Technology limitations
 - e. g. Software requires userid/password



Identity Flow for Transitive Trust

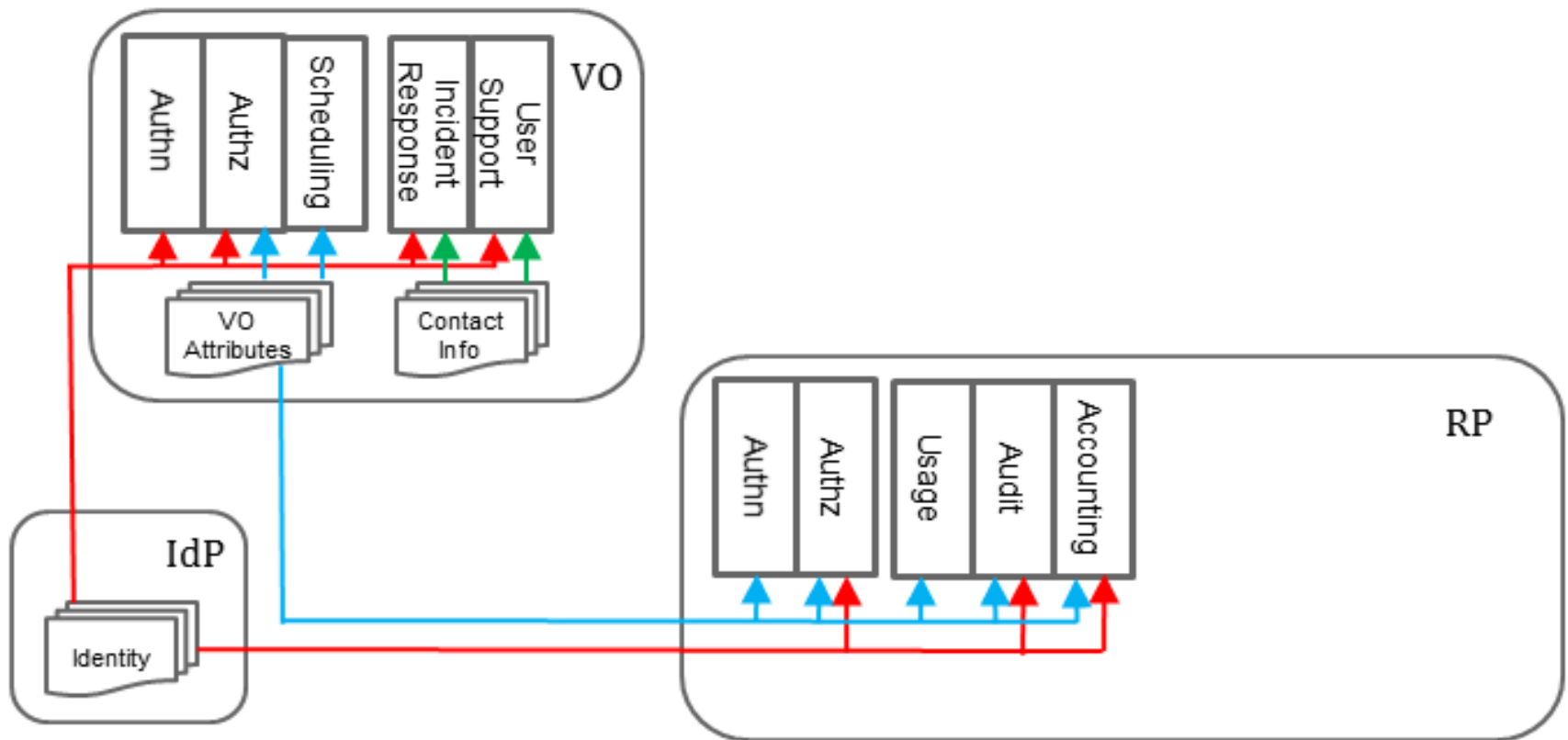


Issues for Transitive Trust

- Lack of persistent personal storage at RP
 - RP is not aware of user identity
 - Data must be staged in/out as part of batch job
- Shared collaborative services
 - Wikis or forums isolated to the VO
 - VO-supplied IdM
- User Support and Incident Response
 - RP has no ability to contact user
 - RP must trust VO to resolve issues
- Roadmap
 - Start with a transitive trust approach (simple) and adjust, as needed, to address particular risks or requirements

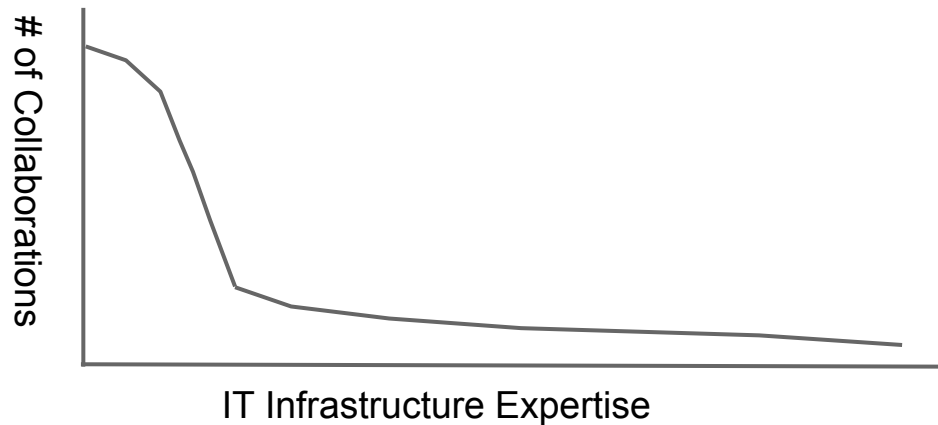


Identity Flow--Modified Transitive Trust



How To Address The Long Tail of Science?

- In the IT infrastructure world it is really a LUMP
- Many collaborations have little/no expertise
- Collaborations need VO infrastructure to adopt
- IdM is part of the problem but not all



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.”
- Efforts funded in the EU such as FIM4R and SCI
 - Federated Identity Management for Research <https://indico.cern.ch/event/301888/>
 - Security for Collaborating Infrastructures <https://www.eugridpma.org/sci/>



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.



**CENTER FOR APPLIED
CYBERSECURITY RESEARCH**

INDIANA UNIVERSITY
Pervasive Technology Institute