Do You Need To Know Your Users?

Bob Cowles, Craig Jackson, Von Welch (PI)

2014 Fall HEPiX Meeting, Lincoln, Nebraska

October 15, 2014

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/VOIdM13

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.

OSG September, 2014 Newsletter. http://www.opensciencegrid.org/managing-access-to-your-virtual-organizations-resources/

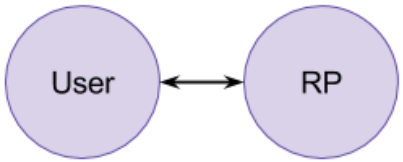
Some Core Findings….

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*.

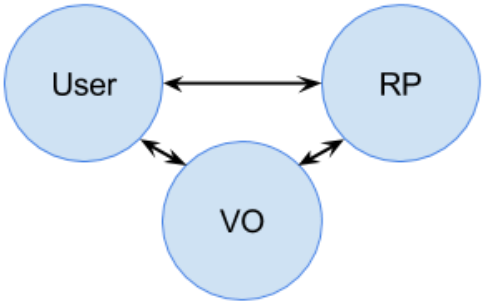
VO IdM Trust Model Extremes

... via 800-39

Classically RPs produced and consumed all IdM data.

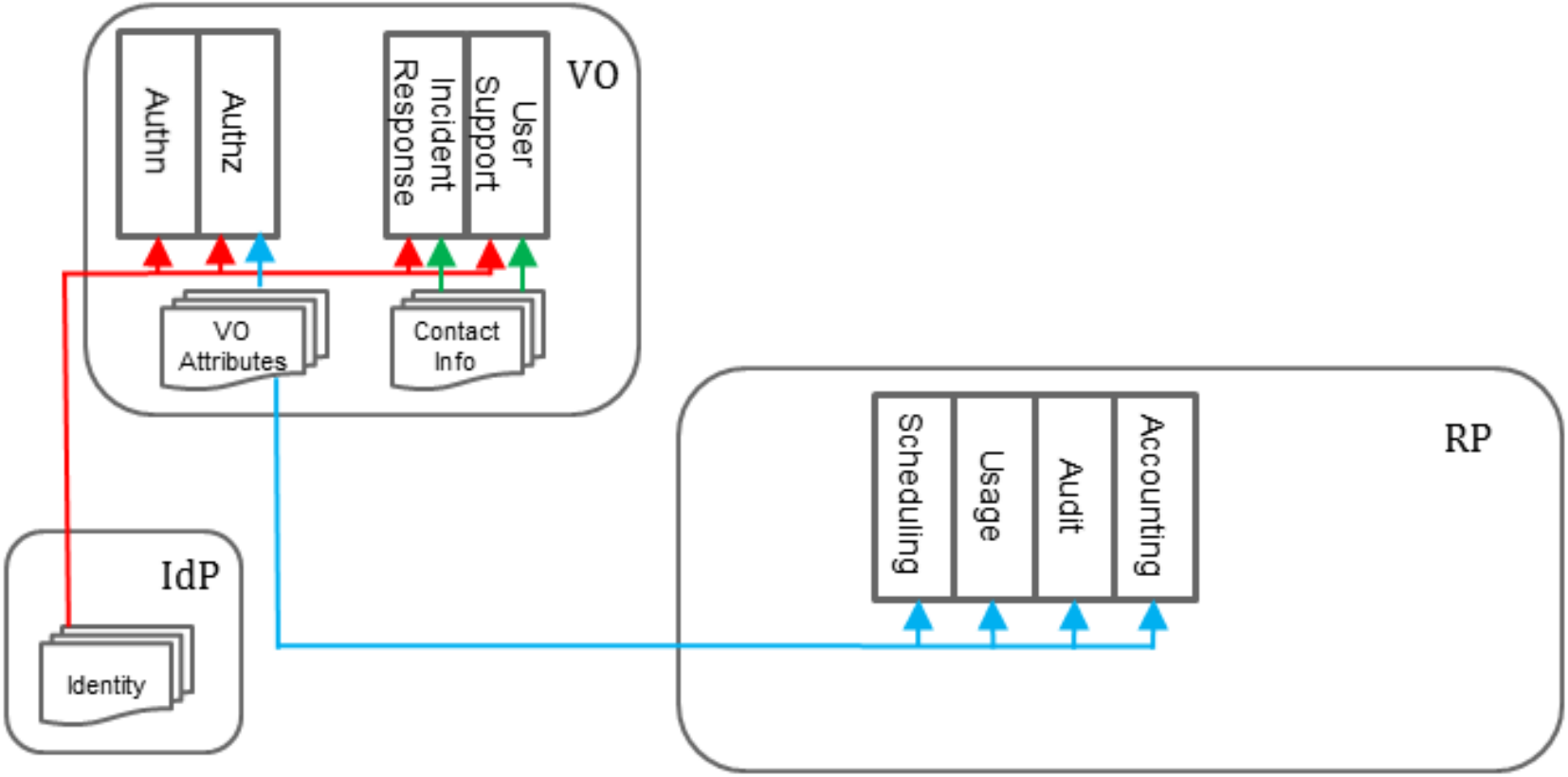


Brokered trust relationships entail VOs & TTPs generating user data, to be consumed by RPs.



Transitive trust relationships forego all user data consumption by RP.

Identity Flow for Transitive Trust



Transitive Trust -> 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

Barriers to Transitive Trust Model

- Compliance and assurance requirements (US)
  - Deemed export regulations
  - http://www.bis.doc.gov/index.php/policy-guidance/deemed-exports
  - DOE Order 142.3 Foreign Visits and Assignments
  - https://www.directives.doe.gov/directives-documents/100-series/0142.3-BOrder-a
- Low risk tolerance and historical inertia
  - "We've always done it this way"
  - Changes risk profile
- Technology limitations
  - e. g. Software requires userid/password

Deemed Export

- "… releasing controlled technology to a foreign person is informally referred to as a deemed export"
- "Release of controlled technology to foreign persons in the U.S. are "deemed" to be an export to the person's country or countries of nationality …"
- "Typical organizations using deemed export licenses include universities, high technology research and development institutions, bio-chemical firms, as well as the medical and computer sectors"

Deemed Export Exclusions

- Research using publicly available information
- Fundamental Research is excluded
  - Fundamental Research is defined as "basic and applied research in science and engineering where the resulting information is ordinarily published and shared broadly within the scientific community"
- Providers of Grid and Cloud Computing Services are not "exporters"
  - http://fismapedia.org/index.php?title=Doc:Application_of_EAR_to_Grid_and_Cloud_Computing_Services
  - "Since the service of providing computational capacity through grid or cloud computing is not subject to the EAR, the service provider is not required to inquire about the nationality of the customer."

Foreign Visits & Assignments (FV&A)

- DOE Order 142.3A - October 2010
- Requires access to DOE Information and Technology by foreign nationals be approved in advance
- More stringent requirements for DOE Labs performing classified work
- Causes some DOE Labs to have restrictive or difficult policies/procedures for foreign national access to scientific computer systems

FV&A Alternate Interpretations

- p.13 “Chief Information Officer (CIO). Drafts policy ... regarding protective measures required for foreign national cyber security access approval, whether onsite or by remote access.” [This has never been done.]

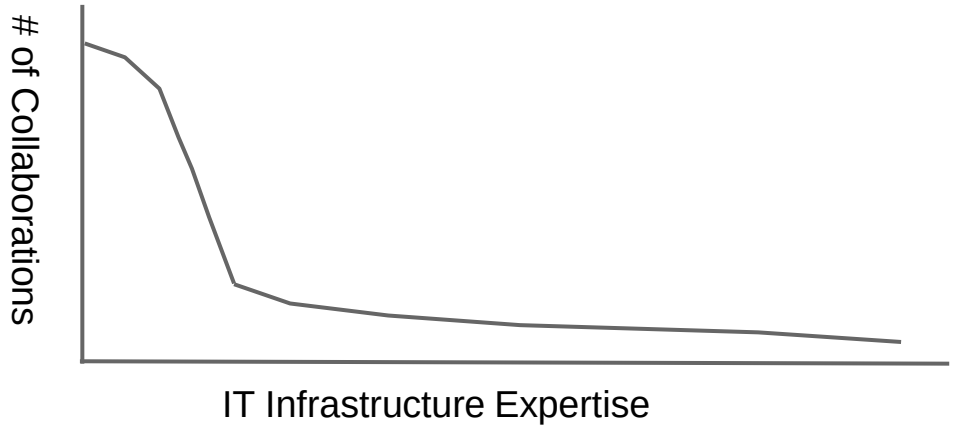
- Graded Approach detailed in Appendix 2: Regarding unclassified work at DOE science labs: “These requirements apply only to those visits and assignments conducted in support of DOE missions and goals, or that otherwise involve access to DOE information or technologies.” [“information or technologies” not “information technologies”]

Changes Risk Profile - Trust the VO

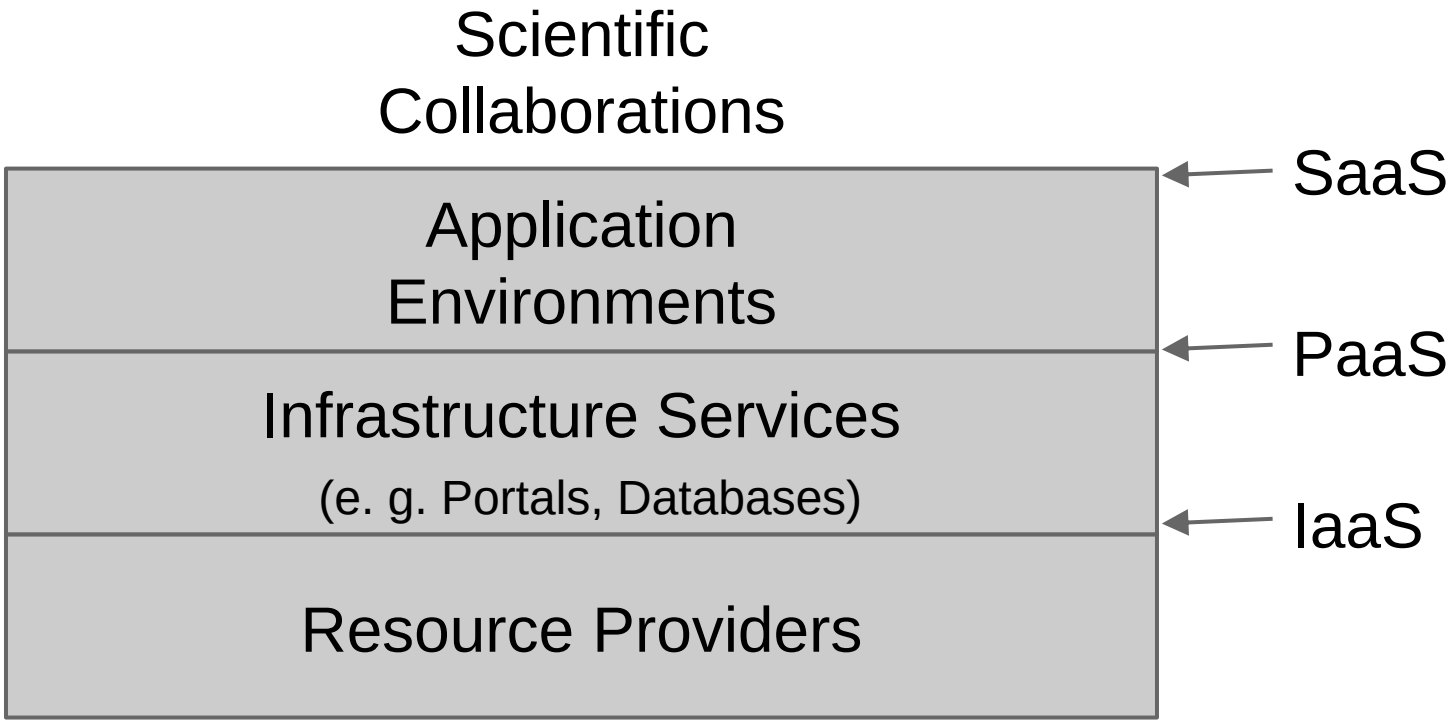
- Many RPs provide user accounts with excessive privileges or access
  - Users no longer need email, individual local storage
- The VO becomes the "user" -- with services provided in a cloud-like model
- Minimal risk so long as services are encapsulated
  - E. g. each VO has a wiki rather than a single wiki for all VOs.

Must 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



Scientific Computing Architecture



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.