

Identity Management Issues

- status and plans

OSG and ESnet

Mine Altunay - FNAL

Mike Helm, Doug Olson, Dhiva Muruganantham - LBNL

International Symposium on Grid Computing
March 2010, Taipei

The Context

- Scientific collaboration typically involves using a collection of credentials of different types with grid (X.509) credentials being just one of many.
- Open Science Grid (OSG) depends on the DOEGrids CA at ESnet for issuing many of the grid certificates used by OSG users.
- Many Users are not happy! The LHC users Are OK – but are they used to the pain?
- We conducted a survey and held a workshop to get a common understanding of
 - What Identity Management (IdM) is
 - How is IdM evolving, generally on the Internet
 - Get VO feedback: what is working, what is not working
 - Identify short& long term action items for our teams

Outline

- How we see the ID Management landscape
- Community requirements
- Survey results
- Conclusions and Action Items

The IdM landscape

- The group:
 - Security Experts: Von Welch (NCSA), Jim Basney (NCSA, myproxy), John Volmer (ANL, DOE PKI), Rachana Ananthakrishnan (ANL, ESG-OpenID), Dave Kelsey (WLCG), Scott Koranda (LIGO)
 - Community representatives: LIGO, SBGRID, Engagement, WLCG
 - OSG & ESNet: security teams and directors
- Considered the issues as ID credentials are used throughout a distributed system from User to ID Provider to Services and Resources.
- Analyzed and compared various system implementations for the characteristics/capabilities that are important for our grid domain.

Comparison of Systems' Capabilities

Systems / technologies

- X.509 IGTF
- SAML – InCommon
- OpenID – ESG
- DOE Entrust (X.509)
- HSPD-12 (U.S. Govt.)

Capabilities / functions

- ID vetting
- Assertion (credentials)
- Revocation
- Validation
- Federation
- Naming
- Delegation
- Lifetime

Comparison Table

(don't try to read it.. Next slides shows key findings..)

| | X.509-IGTF Authentication Digital Signature | SAML-InCommon Authentication | OpenID-ESG Authentication | DOE Entrust Digital Signature Encryption | HSPD-12 Physical Access Logical Access ▪Authentication ▪Digital Signature ▪Encryption |
|-------------------|--|--|--|--|--|
| Vetting | IGTF: face-toface govt ID, RAS network, IDMs CAs run by Grid Projects | Basic: tell us what you do. Silver: face-to-face with govt. ID IdPs run by universities | ESG MOU – Each site agrees to being registration | Paper agreement – each user Common Policy | Background 5 year Fingerprints Photograph 3 people to issue Common Policy |
| Assertion | X.509 End Entity certificate Not targeted | SAML authorization assertion; “Bearer credential” Targeted to an SP | Association over SSL | Common Policy – Soft link | Common Policy – hard link PIV-I PIV-C |
| Revocation | CRLs | ? Short-lived assertions | ? Short lived assertion Nothing explicit | CRLs | CRLs: 30hr, 24hr, 18hr OCSP |
| Validation | SSL Digital signature | Digital signature / SAML metadata | White list of IdP Association via auth channel (ESG requires SSL, signature is optional, noone has done anything else) | | |
| Federation | IGTF International members 50 members. CA validation | InCommon members and growing 150 members. SAML Metadata includes IdPs and SPs. Trust must be both ways | ESG 10 members. ESG ID distribution: IdP Addr and public key SPs must have a trusted certificate. ESG has own CAs. DOE CA is trusted. (General case: anyone can trust anyone.) | Common Policy – Soft link | Common Policy – hard link |
| Naming | CA have unique name spaces | ePPN: jbasney@illinois.edu eTID: x9738yz@illinois.edu | OpenID in context of IdP | Department of Energy | U.S. Government |
| Delegation | Proxy Certificates | Some proposals | Not used, can be used with OAuth | | |
| Lifetime | 1 year to 1 week | minutes | ? | 3 yr | 3 yr |
| | | | | | |
| | | | Google, Facebook are providers | | |

Systems / technologies

- X.509 IGTF
 - X.509 based grid credentials as used by OSG/WLCG
- SAML -InCommon
 - SAML based Shibboleth as used by the InCommon Federation of Higher Ed. in U.S.
- OpenID – ESG
 - OpenID as used by the Earth Systems Grid
- DOE Entrust (X.509)
 - X.509 infrastructure use by U.S. Dept. of Energy headquarters
- HSPD-12 (U.S. Govt)
 - Smartcard ID system used in U.S. Federal govt.

Capabilities

- **ID vetting**
 - Process of establishing identity and assuring that credentials are issued to correct person
- **Assertion (synonym of credential)**
 - The token that makes an identity claim about a person or an entity and is used to authenticate a transaction
- **Revocation**
 - Ability to remove the validity of a credential so that it will fail an authentication/ authorization test
- **Validation**
 - Action to establish if a particular credential is valid (OK to use it)
- **Federation**
 - An associated group of ID and service providers with a common policy that will accept/interchange credentials
- **Naming**
 - Policies for name uniqueness and required attributes in credentials
- **Delegation**
 - Generation of a child credential from a parent credential when an action crosses boundaries to additional services that require authentication/authorization
- **Lifetime**
 - Ability to establish a valid lifetime for a credential and take appropriate action when credential expires

Key results of comparisons

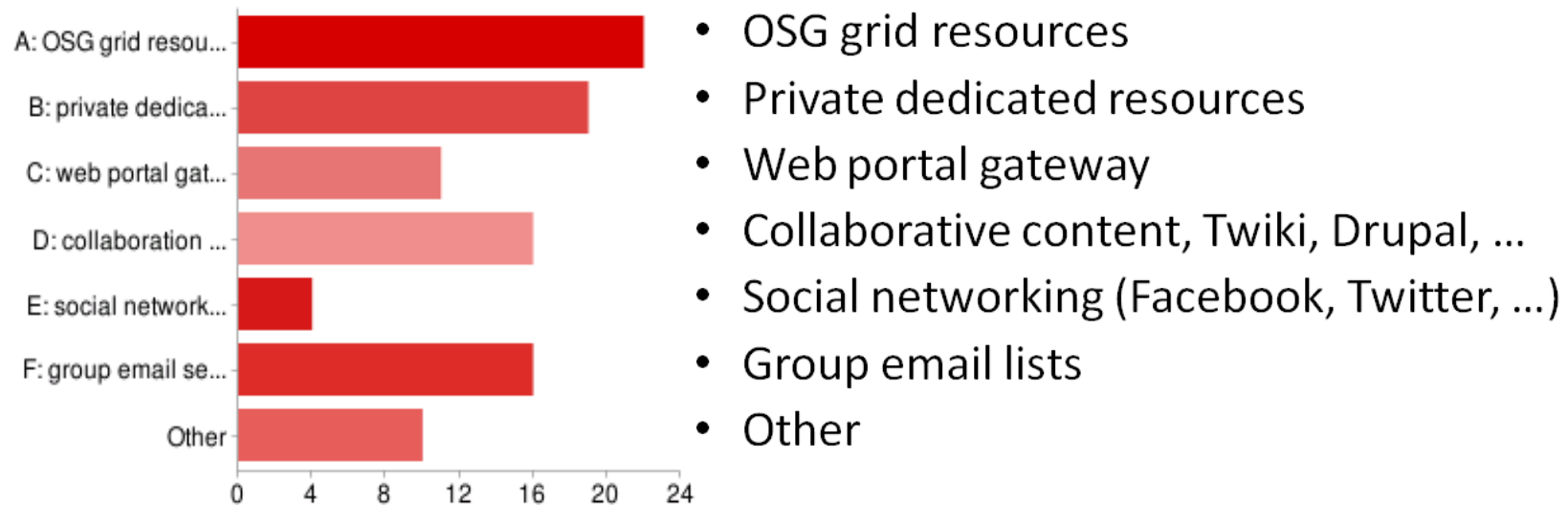
- **Delegation** is an essential capability for long-running grid jobs and is the key feature of X.509 proxy certificates. Delegation in the web protocols (Shibboleth, OpenID) is used somewhat at interactive timescales but not currently in a form suitable for grid use and timescales.
- A **Usability Gap** exists between the web client interfaces and existing grid, unix shell, interfaces. There is no unified access control model. It is awkward to move credentials between domains. It is hard to manage certificates on user's desktop.
- **Federation trust** is secured with X.509 PKI, even in web domain (SSL certified trusted sources of metadata).
- User and developer communities in the web domain are much larger than in grid domain so there is likely benefit to **leveraging web developments** for grid tools.

Community Requirements

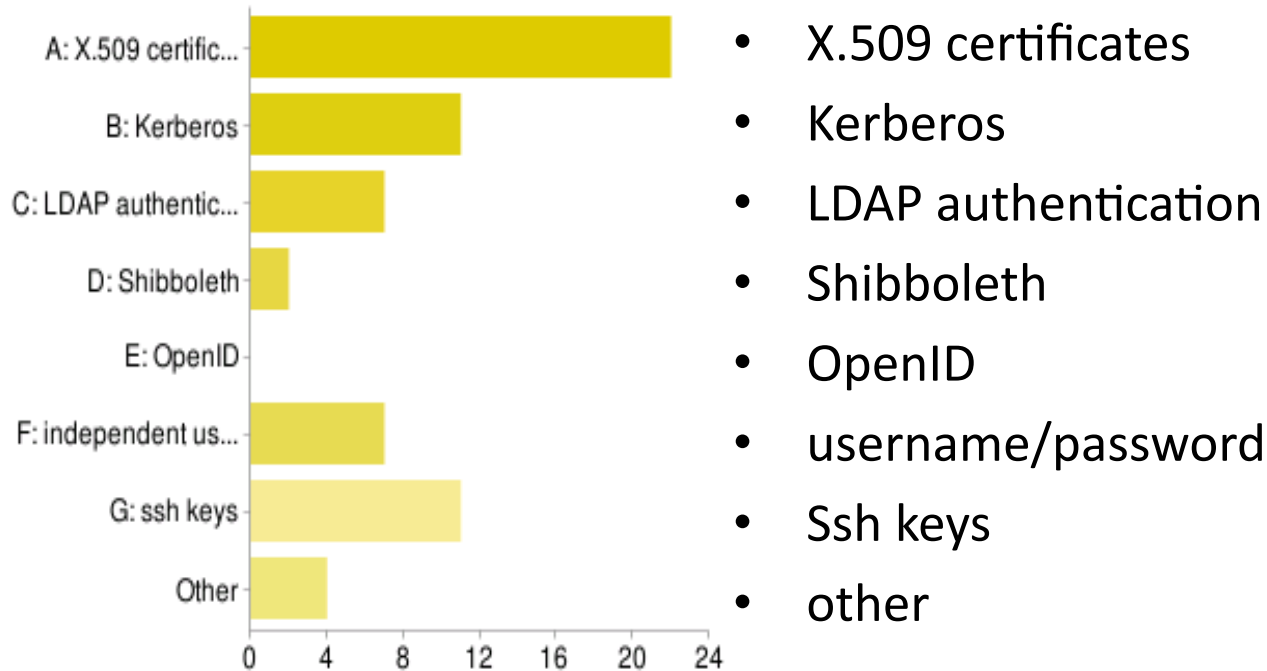
- Collected from representatives of 8 VOs during the workshop, and 17 VOs replied to online survey
- 8 *happy* with current implementations
- 7 need **single-sign-on-like** environment for scientific (grid) and collaborative (web tools) work. Unified access control across web and grid.
- 17 (all VOs) very frustrated with the **usability gap on the desktop for handling credentials** across web & grid domains.
- Need a better integration of certificate registration and HR (membership management) functions currently dealt with by the VO.
- Support for smaller dynamic VOs is a need
 - **light-weight**, intuitive (like uname/passwd) access control similar to web-based apps. **Shorter time** to get credentials and start working on the grid. Currently difficult in the OSG model and technologies we use.

Details of Survey results

- Responding groups:
 - Fermilab, LIGO, OSG, nanoHUB, DES, DOSAR, ATLAS, Dzero, SBGrid, CompBioGrid, ALICE, CDF, CIGI, IceCube, CMS, Engage, STAR
- IT/CI resources used for all aspects of collaborative work

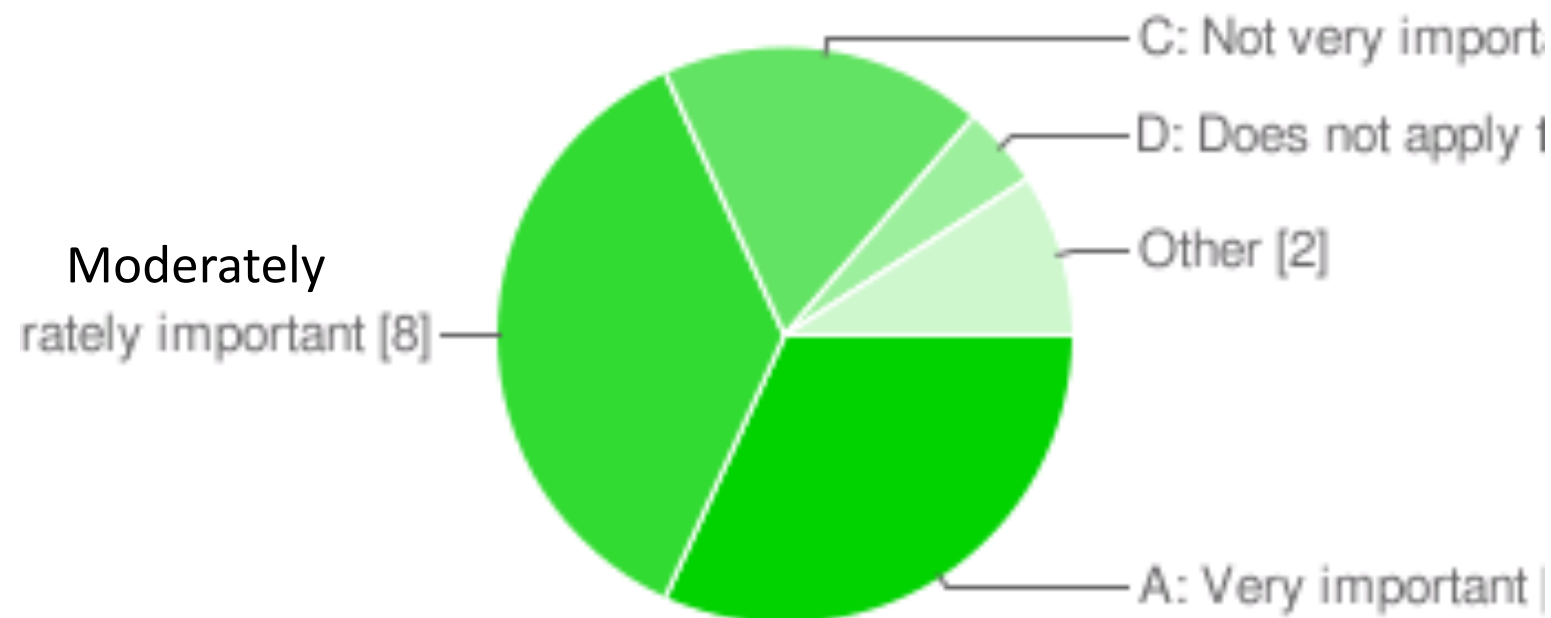


Authentication methods used VO-operated services/resources

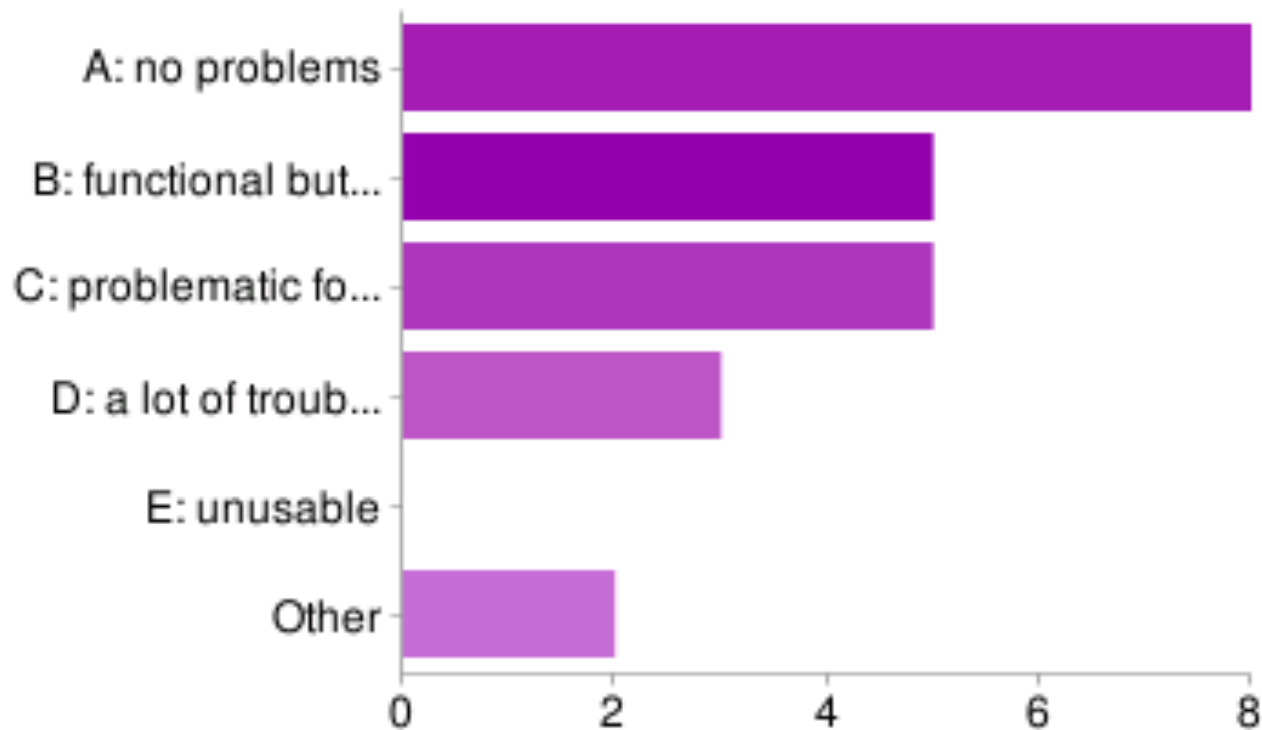


The X axis shows the number of VOs, y-axis shows the access control mechanism employed by that many VOs.

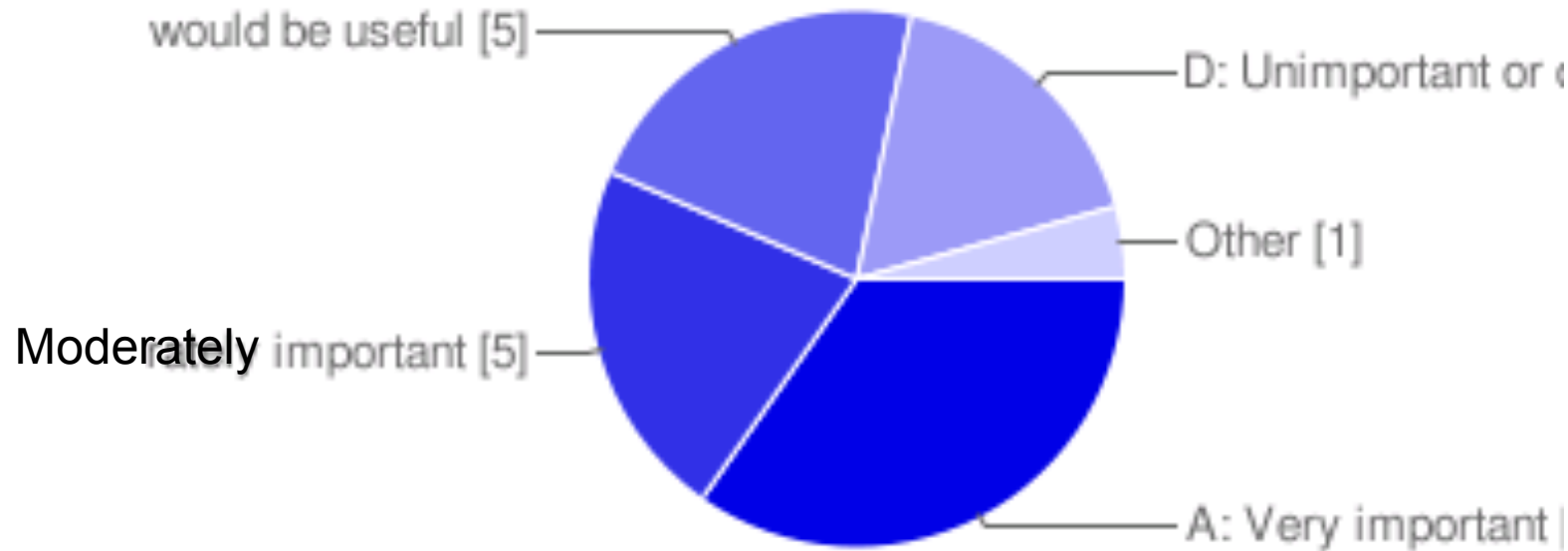
Access web portals with grid credentials



Issues using certificates with web browsers, unix shell, email (smime)



Importance of integrating grid credentials with other authentication methods



Importance of having the DOEGrids CA trusted by browsers and email clients by default

- Moderate importance, importing trusted CA certificates is annoying but people manage 39%
- Not important, better to improve other aspects of the service 4%
- Extremely important, many people fail to import CA certificate and mark it trusted 30%
- Very important, many people have trouble installing trusted CA certificates 22%
- Other 5%

Conclusions and Next Steps

- Existing IdM systems are **functional** for current grid users, but **have issues** and also **inhibit** infrastructure adoption by **new users**.
- Easy-to-use **certificate life-cycle management tools on user's desktop**
- Have a **unified access control** across web domain and grid domain, and take advantage of **web domain technologies** in future developments.
- Any solution should allow for **VO-wide single sign-on** to VO services

Current Actions

- Usability on user's desktop
 - All VOs suffer from this.
 - Find tools to manage certificate lifecycle on user's desktop: request certs, export/import from/into browser, email clients, unix shell, move credentials across user desktops, renew, revoke...
 - It is a hard problem -- diverse OS and browsers

Current Actions

- Examined certificate tools from European CAs – e.g. NIKHEF CA, UK e-Science CA, CILogon CA, Fermi KCA
 - None solves the problem completely – usually focuses on a OS/browser
 - UK e-Science: Java web start, file mgmt, MyProxy upload, browser import, voms- proxy-init, CA roots import
 - Fermi KCA: shell script for retrieval, file mgmt, browser import
 - NIKHEF CA: JgridStart, request, retrieve, import into browser, file mgmt

Current Actions

- Having each CA develop their own tool the answer? What if users have multiple certs?
- Web apps do not continuously run on desktop and check for expiry, renewal, errors and such.
- Should we have a generic client tool distributed by middleware and ask CAs to configure against it?
- Is this a losing battle with ever changing OS/browsers? Maintenance, support?
- Could solve the problem for browser and grid clients but what about other services that does not use certificates? How to integrate access?

Current Actions

Consider the private key management for the end user

- Move the certificates away from the desktop and store them at a professionally managed service for the user
- New private key user guidelines allow for it. More secure than user desktop. Short-lived certificates would be the choice
- Username/password for accessing the private key store

Current Actions

- Becomes a complete solution when the same uname/passwd is used for the web resources
- Would ease single sign-on across all VO services
- Burden is on the VO to run another uname/passwd repository. But VOs already perform the ID vetting so not much difference here
- Single point of failure?
- Compromise of the uname/passwd repository would bring the whole VO down. But so does the VOMS compromise

Current Actions

- Supporting small/dynamic VOs
 - Short light-weight user bootstrapping, get grid access in 30 minutes
 - Streamline VO and Certificate Registration
 - Worked with SBGrid to reduce 8-step process
 - Make sure VO admin is also RA Agent
 - Get the certificate and get instant membership in VOMS
 - Could benefit from Federation-CAs to get instantaneous certificates, but there are few institutions that provide IdP interface
 - Certificate vetting still needs to be manual, out of the band, could take a few days

Current Actions

- If we decide to move user away from certificates and position VO as the IdP
 - VO can decide to join federations and interact with other IdP and Sps.
 - VO can have more say and more direct exposure to federations
 - Is this better than having shib-enabled CAs?
- Many options to discuss.
- We will present at OSG AHM at 3/8 and make a longer term plan