OSG-ESnet Joint Identity Management Workshop,

9-10 Nov. 2009, Madison, Wisconsin

M. Altunay, M. Helm, D. Olson, and D. Muruganantham

DRAFT 3, 8 Jan 2010

Contents

Executive Summary: Steps Forward

This workshop had two goals: an assessment of the identity management landscape from a computer science perspective, and then gathering user feedback on the current security infrastructure.

Usability is found to be an afterthought and hence a challenge in our infrastructure. All of the VOs identified **lack of certificate management tools on the desktop** as a serious problem in terms of **end user experience**. After a user is approved for a certificate, she has no means to manage the certificate life cycle: exporting/importing certificates, configuring a certificate for Unix shell access, transporting certificates to a different computer, importing certification authority (CA) trust roots, and so on. These activities become very frustrating for users, especially for a grid beginner. The lack of usability has negative consequences from a security perspective in addition to general unhappiness of the users: users may invent work-arounds to avoid impediments of the security infrastructure (e.g., remove passwords from private keys) resulting in different vulnerabilities. It is likely the desktop problem as stated is not solvable by organizations like ESnet and OSG alone. We will have to look at how we can present alternatives that we can manage. Providing short-term (ephemeral) PKI credentials is one alternative but will not meet every use case. Looking at "credentials in the cloud" or an online service for credential stores, and hiding all the PKI and token movement operations in an API, is another alternative that should be explored more thoroughly. While it is likely that significant change will not be easy, and perhaps not even accepted by physics experiments at the current time, many **other disciplines seem to need more flexible as well as less cumbersome identity services**. There are technical challenges as well as policy and security challenges to face.

A new web-based flavor of collaboration tools. such as wikis and e-logs, has emerged, and been used by the scientific communities. All of the OSG VOs report using web-based collaboration tools. For LHC VOs, the tools are not critical for achieving the science goals. Non-LHC VOs, however, report a more rapid adaptation and attach higher criticality to such tools. These new tools have a different access control model than that of grid computing tools. This means that an end user should manage multiple identities and learn to switch between the identities based on the used tool. This is difficult for the end user. The trend among the non-LHC VOs is to design a VO-grown, upper-layer identity management infrastructure that can unify access across all of the VO tools. This is a significant undertaking for the VOs and consequences should be understood by OSG, ESnet and VOs all together.

Interactive (web-based) vsversus. non-interactive (batch/grid) computing models use different access control models. The identity management systems that are built for the web-based tools expect an interactive computing environment, where continuous user presence is assumed. Whereas, the grid is modeled for long-running batch jobs, where no such assumption can be made. Grid credential delegation, a key feature of grid infrastructure, enables the long-running batch jobs. However, delegation does not exist in the same form or degree in the web-based domain although n-tier models and cloud computing have use cases moving in that direction. This makes it difficult to adopt web-based identity management tools in grid infrastructure.

Nevertheless, the web-based tools reach a far higher number of users than grid does and thus they help shape the IT industry standards. Moreover, grid users benefit from the web-based tools as well. **Our conclusion is to continue evaluating the web-based identity management systems and investigate feasible ways to merge them with grid identity management. The OSG security team will design an end-end identity management system prototype that includes web- and grid-based tools.** This design will be a first step to understand the differences and similarities in depth. **ESnet will continue to study and prototype internet identity protocols (such as SAML and OpenID) and explore techniques for interoperating these protocols with DOEGrids PKI and other commercial services. In addition we should participate in the new initiative focused on improving the trustability of OpenID and CardSpace – based identity providers.** Successful development of the "TFPAP" initiative will remove substantial security barriers to adoption of these simpler protocols.

Non-LHC VOs unsatisfied with the current PKI-based grid infrastructure have expressed a desire to use alternative identity services (and in some cases they have acted on that desire). OSG and ESnet should more thoroughly understand the reasons for this dissatisfaction. User frustration with certificates - the usability and the desktop problem as described above – is often cited. There may also be organizational or project-related drivers. ESnet and OSG PKI is one implementation of PKI out of many possibilities; it may be that alternative approaches to PKI will meet some projects' needs. Before making grand architectural changes, it is essential to understand project issues better. **We need a regular process of dialog and discussion to assess the OSG infrastructure. Building and maintaining such a process is an action item for OSG, ESnet and VOs.**

Improving the user experience of the existing PKI services would be a great benefit, so long as existing processes are not disrupted. Reducing the burden of the desktop problem, and reducing the amount of manual key management expected from users are clearly desirable from a user's point of view.

OSG defines improving usability and desktop problem as action items from this workshop.

So far ESnet and OSG have limited their efforts to grid infrastructure, other types of collaborative tools have mostly been treated as out-of-scope. Now is a good time for both organizations to evaluate this position. By designing a prototype end-end identity management system that includes diverse collaborative tools, OSG takes the first step in expanding its horizons. The results from this design help OSG assess its further steps. **ESnet is planning to hold another workshop to gather requirements from the broader community of ESnet stakeholders. That workshop will be helpful in evaluating the scope and future plans**.

Goal 1: Living in an Evolving Identity World

The goal of the first day session was to lay out a conceptual identity management diagram that all of the attendees could agree on. Later, based on the diagram (Fig 1.), we discussed and compared different technologies.

A Conceptual Diagram of Identity Management

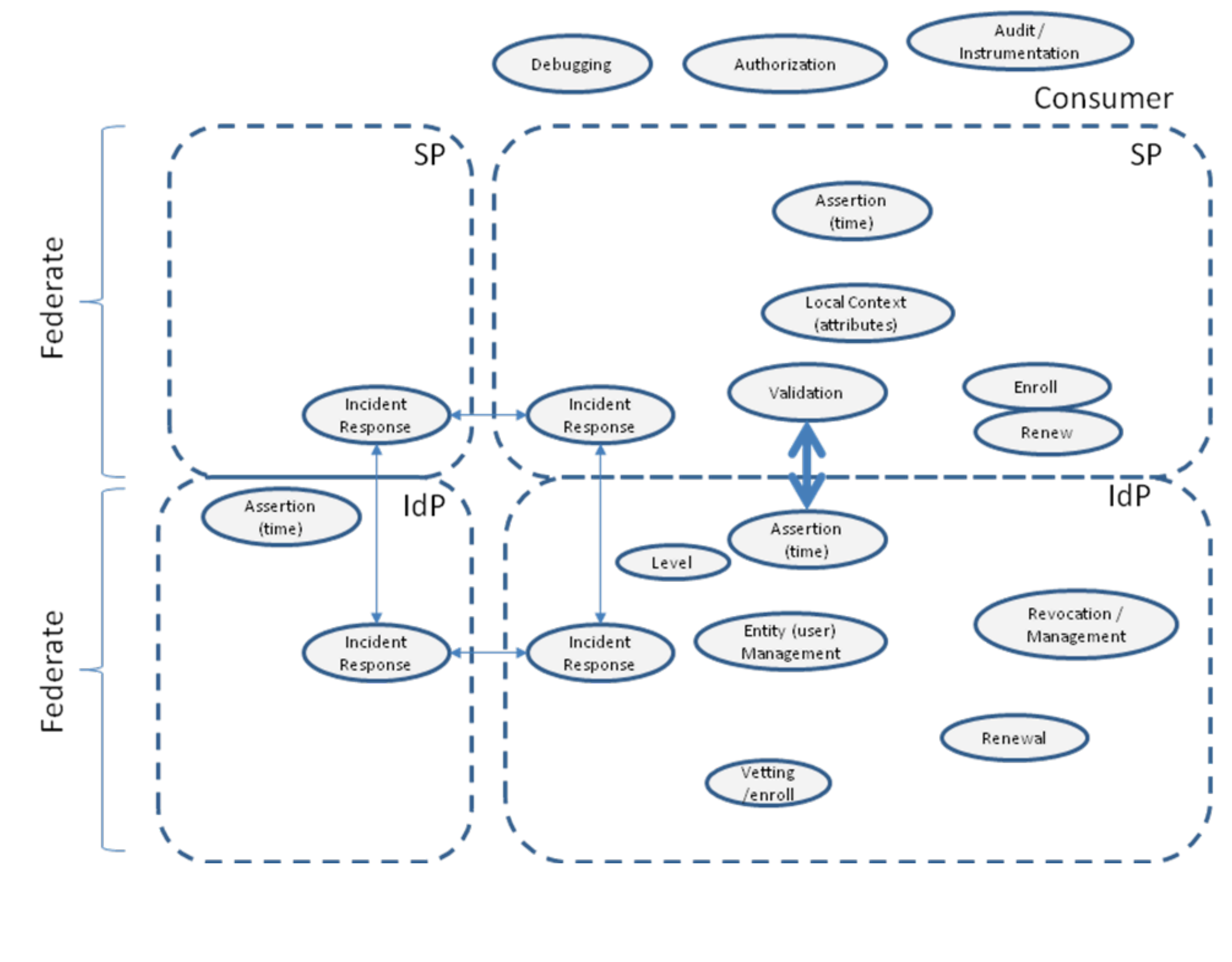


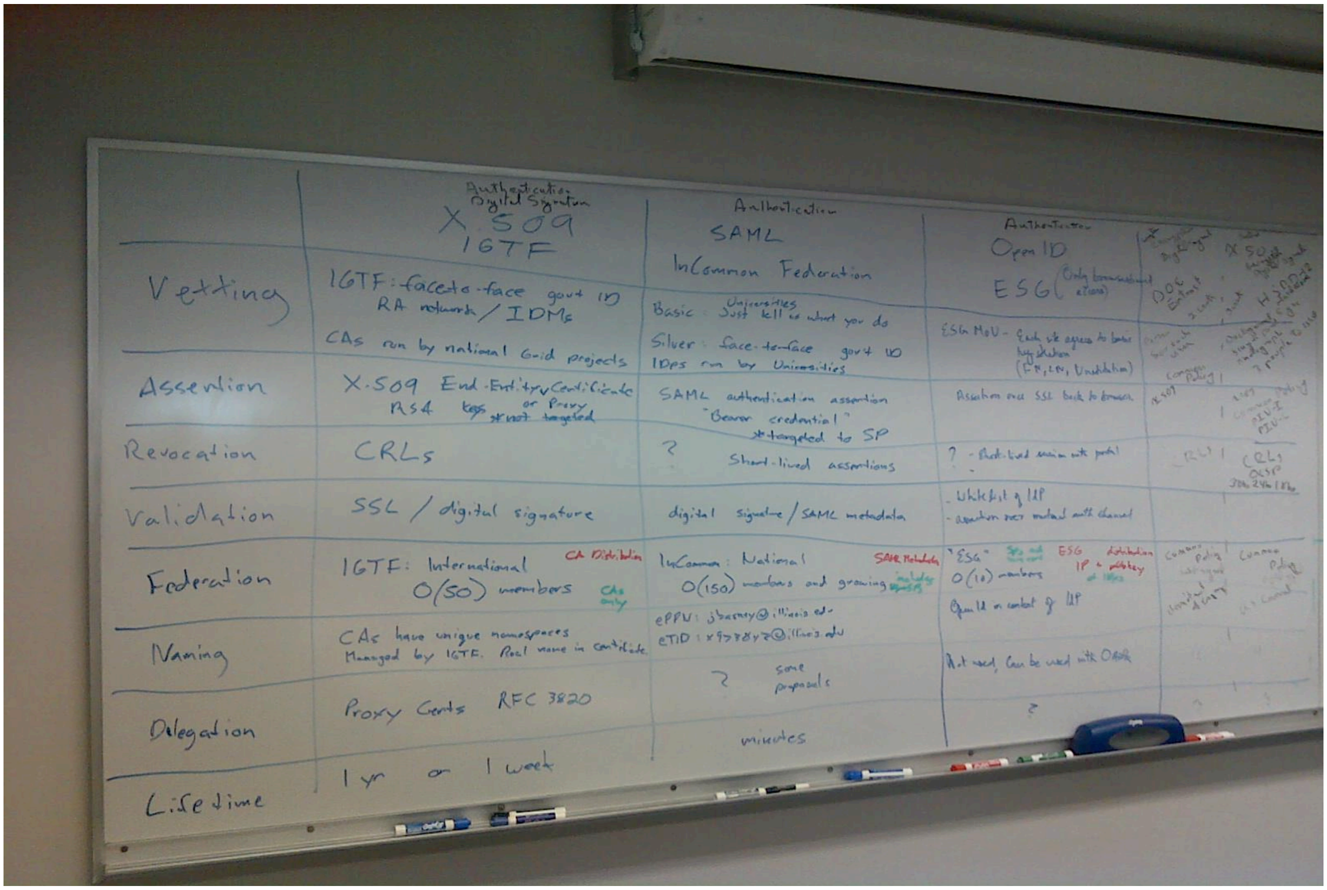
Figure 1. A Conceptual Diagram of Identity Management1

We agreed to use the term "*assertions*" instead of certificates, credentials, etc. An assertion is a unique statement about a person's identity. An X.509 certificate, for example, is implementation of an assertion.

- Incident response is a common element that is repeated at SP and IdP layers. Moreover, it is used between separate IdPs as well. We sought for any other common elements between IdP, user, SP or federation. Our argument did not include much in detail how this diagram changes when we add separate federations.

- We identified that revocation in the authorization layer (top layer in Fig. 1) is necessary. The revocation here means negating/changing/re-evaluating the authorization decision by rechecking whether the assertions used to make that decision are still valid. Assertions and the authorization decisions tied to those assertions can be treated as two separate control channels. It is a policy decision how to treat them when one of them expires. When an assertion expires, should one leave the authorization decision as-is, or re-evaluate the decision, or negate the decision and undo all past actions allowed by that decision, and so on.
- Propagation of assertions in the middleware and the infrastructure is needed. Would propagation of an assertion be equal to creating a new assertion? We have not reached a conclusion.
- Users' ability to scope their assertions is a needed piece in identity management. A user can pick and choose the assertions about herself.
- We agreed that users are often an after-thought in the security systems, and usability is not a driving concern for the security architectures.

Discussion of Existing Technologies against the Conceptual Identity Diagram



	Authentication Digital Signature X.509 IGTF	Authentication SAML InCommon Federation	Authentication Open ID ESG (Only browser-based ations)	[illegible] Dig Signat DOE Entrust 3 certs	X.509 [illegible] HSPD12
Vetting	IGTF: face-to-face govt ID RA network / IDMs CAs run by national Grid projects	Basic: Universities Just tell us what you do Silver: face-to-face govt ID IDPs run by Universities	ESG MoU - Each site agrees to basic registration (FN, LN, Institution)	[illegible] Common Policy	[illegible] 3 people to issue
Assertion	X.509 End-Entity Certificate or Proxy RSA keys *not targeted	SAML authentication assertion "Bearer credential" *targeted to SP	Association over SSL back to browser	X.509	X.509 Common Policy PIV-I PIV-C
Revocation	CRLs	? Short-lived assertions	? - Short-lived session with portal	CRLs	CRLs OCSP 30hr 24hr 18hr
Validation	SSL / digital signature	digital signature / SAML metadata	- Whitelist of IdP - assertion over mutual auth channel		
Federation	IGTF: International O(50) members CA Distribution CAs only	InCommon: National O(150) members and growing SAML Metadata	"ESG" O(10) members ESG distribution IP + pubkey of IdPs OpenID in context of IdP	Common Policy	Common Policy
Naming	CAs have unique namespaces Managed by IGTF. Real name in certificate	ePPN: jbasney@illinois.edu eTID: x9>78yz@illinois.edu ? some proposals	Not used, Can be used with OAuth		
Delegation	Proxy Certs RFC 3820		?		
Lifetime	1 yr or 1 week	minutes			

A table of existing technologies against the conceptual identity diagram.

	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
Revocatio n	CRLs	? Short-lived assertions	? Short lived assertion Nothing explicit	CRLs	CRLs: 30hr, 24hr, 18hr OCSP
Validation	SSL Digital	Digital signature /	White list of IdP		

	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
	signature	SAML metadata	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		

Delegation

- X.509 provides offline delegation; necessary for non-interactive long-termed batch jobs to run.
- SAML and OpenID protocols do not provide delegation. This is a huge drawback for their usage in the non-interactive grid world. But any technology can enhance the protocols and/or implement the delegation. Current SAML work on delegation is not scalable, and, designed for interactive online systems. The delegation request always goes back to the IdP
- Oauth1 is an authorization protocol for the web applications.

Interactive versus. non-interactive work environment

- The web world is built on the assumption of interactive usage model; grid is built on the non-interactive usage model. Grid jobs are long-termed batch jobs with no expectation of user interaction. Web world needs and desires user interaction because the application lifetimes are much shorter and the service providers desire to keep the customer on their web site actively.

[1] http://hueniverse.com/2007/10/beginners-guide-to-oauth-part-i-overview/

- Most solutions like SAML and OpenID are designed for web and will not meet grid world's needs. Should grid world abandon its access model and follow the rest of the world? What would grid infrastructure look like if we assume it is purely made by web protocols?
- Would the web world eventually evolve into the grid world direction and require non-interactive usage models?

Privacy

- The disclosure of user DN's are required by IGTF and the compute elements. Would there be any consequences in terms of privacy, especially in trust federations?

Usability

- The user interface of Shibboleth or OpenID login is identical to the interface of a phishing attack; the user goes to a central web site and then clicks on a link to log in to their home organization. An attacker uses the same scenario, except she would not forward the user to the real home organization's web site and would also steal the user's username/password. It is alarming to get grid users accustomed to being forwarded to their home web sites for login. (Actually a good thing)
- In order to eliminate MITM and phishing attacks, the end user and the providers should use SSL, hence certificates. Importing the CA trust roots and paying attention to ssl connection would be a burden on the user.
- In order to join a trust federation, providers should also present certificates. Thus, trust roots in a trust federation like InCommon is essentially the Certificate Authorities that this federation trusts.

Goal 2: OSG User Communities' Requirements from Identity Management

USATLAS, USCMS, LIGO, Alice-USA, OSG-Engage, Fermilab, and STAR VOs attended the requirement gathering workshop. A questionnaire of identity management issues have been sent to all OSG VOs. The results of the survey are available at http://spreadsheets.google.com/pub?key=t429dxm3_5SJyRexugOsBNAandoutput=html.

Usage of DOEGrids CA certificates: User Experience in Certificate Life Cycle.

- DOEGrids CA infrastructure mostly suffices for the needs of VOs whose usage model is non-interactive grid jobs, namely CMS, ATLAS, Dzero, CDF, and Star. There are areas of improvements to DOEgrids CA infrastructure, but the basic functionality is working well.
- VOs that rely on web tools, non-grid based production mechanisms, or tools with diverse authentication mechanisms are significantly unsatisfied with the DOEGrids CA infrastructure, namely SBGrid, LIGO and CompBioGrid.
- It is not clear whether unsatisfied VOs' needs can be fully met by a PKI infrastructure; or whether the problem is due to the particulars of the DOEgrids CA infrastructure.
- All of the VOs, satisfied and unsatisfied with the current infrastructure, suffer from the **lack of credential management on the desktop**. We identified user desktop as the *no-man's-land* because neither OSG nor DOEGrids CA offers any tools for managing certificates on the desktop. Once a user is issued a certificate, she is responsible for importing/exporting the certificate, converting certificate format, importing trust roots, renewing, porting the certificate to a new machine. Switching computers or switching browsers is a big problem for end users. Bootstrapping certificate usage is a heavy burden for the user and user is left without tools. Diversity of browsers and OSes also exacerbates the problem.
- Although all VOs complain about certificate bootstrapping/desktop management, some do more for their members than others: this was a sufficient reason for LIGO to switch to a system where end user is completely isolated from certificate handling, whereas CMS and ATLAS users have not felt the need for such a drastic change. It is unclear how much of LIGO's transition is propelled by their dependence on web-based tools. LIGO security contacts rated wiki tools as much as if not more important than grid job submission tools. A unified authentication method across diverse applications, such as wikis, software repositories, etc, was rated as a significant driver for the change in LIGO. Similarly, an average SBGrid user has 4-5 different identities, and SBGrid is interested in having their own CA (similar to LIGO plan). ATLAS and CMS on the other hand do not use applications with diverse authentication methods, and currently have no further requirements from OSG on identity management.
- However, we have not yet fully understood the differences between satisfied and unsatisfied VOs: whether the cause of frustration is related to usage models, user profiles, expectations, or a mix of many other elements.
- We recognized that a side effect of each VO operating their own CA is that each VO becomes an IdP. This could be cumbersome because a person with multiple VO memberships will get as

many identities. The identity as we operate now is not tied to a group membership, but to an individual's legal name and a key pair.

- Fermilab VO had similar problems too, but they have mostly solved them. Fermilab ties a single user identity to multiple assertions. It uses a desktop client to generate certificates and manage them on the desktop. It issues multiple certificates for the VO members. The Fermilab KCA can continue functioning even if Fermilab is off the network. Similar architecture is designed for CDF with Fermilab support.

VO's experience with DOEgrids CA and PKI infrastructure

- Each VO has to participate in the identity vetting process actively. DOEgrids Registration Authority relies on VO members (sponsors) to vouch for a requester's identity. This is a time-costly manual process, often executed via emails. Because sponsors are drawn from different institutions, it is complicated for large VOs. CMS has a worldwide certificate team specially designated to act as sponsors. Furthermore, a VO needs to manage the users' memberships actively; removing inactive users from membership list. All of these efforts resemble **a Virtual HR for a VO.** Every brick-and-mortar organization has an HR, thus should a virtual organization have a virtual HR?

Projected VO Growth, Worst-Case Scenarios (what keeps you awake at night) and Risk Analysis (what can't you live without)

- LIGO expects 10% growth in community and more diversity. Chinese researchers recently joined LIGO. Which Cas are going to be used by Chinese is open for discussion. LIGO is considering IGTF approval of their own CAs. LIGO is gearing to open up its data. External collaborations with gamma-ray researchers are developing. This means restricted sharing of data and joint co-analysis. Thus, finer-granularity data access controls may be needed. Getting their collaborators up to speed is a concern for LIGO.
- CMS expects a factor of 2 user growth. Computing model is not changing. Tier 3 is a bit more dedicated effort.
- For LIGO, the biggest threat is an insider job, a disgruntled student. For ATLAS, grid-targeted attacks are the biggest threat, small scale attacks intrusions. For SBGrid data and process privacy is very important. If VOMS compromised, that is a failure scenario. For CMS, hadoop would be a central failure point. All worker nodes would be lost.
- VOs are asked to think through their worst-case scenarios and risk analysis. All VO representatives agreed to send such a report after the meeting.
- Not the intrusion itself, but the time to clean up and bring the machine back up again are the main worries. This should be better understood.

Sites' experience with DOEGrids CA and PKI infrastructure

- Shortage of CRL lifetimes is causing a headache for the site admins. CMS estimates 1 hour compute time is wasted each day on average due to CRL failures. All resources suffer from this regardless of which CA they use. (not relevant to DOEGrids?)
- The root-cause of this problem is that our middleware implements a common unwritten IGTF policy without giving the other parties an alternative. It suggested to update CRLs every month,

but a CA or a resource may increase or decrease the accepted CRL lifetimes based on their own policies.

Small Dynamic VO Groups

- Quickly forming small VO groups is requested by SBGrid and LIGO VOs (and sns VO although it is not an OSG member). SBgrid needs dynamic groups for data access, rather than computing access as they are sharing http passwords currently. Delegation or assignment of VO management attributes, dynamic creation and propagation of newly-formed VOs, and dissolution of VOs need understanding. Currently there is not a ready solution.

Pilot Jobs

- Do pilot jobs need special access requirements? Do we need to authenticate/authorize pilots any differently than other jobs?
- Site view on the topic (Keith Chadwick) is no; pilots do not need any special access requirements than any other jobs.
- Whether in future each user will run her own pilot jobs?

Storage Access Control Model

- Privacy versus. integrity needs.
- ATLAS needs data integrity, whereas SBGrid and CMS require data privacy. SBGrid is on the hook for scientific privacy needs. They need data and process privacy; the need is valid for non-HIPAA (Health Insurance Portability and Accountability Act) bound scientists as well.
- There is a real need for data access to be managed at group level. Data and computing access models are different: data needs groups, jobs do not need groups. uid is currently used for data access. (CMS data is read available.)

Recommended/Sanctioned Activities

- Both VOs and sites need a list of recommended sanctioned activities in OSG.
- Sanctioned activities, “ten commandments” of grid security. For example, how often to renew a proxy, or how to use a service certificate
- There is a need for having processes for the users to inquire about sanctions, recommendations, challenging earlier decision. Currently a VO or site can contact OSG security team for a recommendation. OSG should advertise the processes more widely.

Comments and Observations

Identity versus Authorization

Alan Karp and Marc Stiegler have been making an interesting case:

(1) There is too much emphasis on identity and related authentication decisions and

(2) There are a set of laws or principles behind collaboration, and most systems don't follow all of them

Because of #1, we spend too much time on identity issues and not enough time on how to authorize an action efficiently. Because of #2 - better said, because not all the principles are followed, users find services frustrating, resulting in various kinds of work-arounds, noncompliance, or failure.

We should take the time to read/listen to their arguments and see to what extent it is usable in refactoring what we are doing.

[MS identifies 6 principal features of collaboration:

Dynamic

Attenuated

chained

accountable

Cross domain

Recomposable

Look here for "Rich Sharing on the Web": http://www.hpl.hp.com/techreports/2009/HPL-2009-169.pdf which explains them and provides examples.]

Security versus Usability

We had several security versus usability discussions during the workshop. It seems to me there is another degree of freedom here, which is complexity. Security and usability often interact poorly and the result of this turbulence is often additional complexity in the application. (Several easy examples can be found in DOEGrids CA). Usually, complexity reduces security by adding more opportunities for errors at various levels, and likewise reduces usability in similar ways. We missed an opportunity to identify complexity as an issue in the workshop but I see it as a serious, undermining problem in federation (can discuss examples). I don't think it is likely that security experts can become usability experts or vice versa very easily. I don't understand what "usability" really is / isn't (and see below), nor do I like security discussions very much as I have said at other times. I don't think either is easily measurable. But maybe, we can measure complexity.

OpenID is NOT the only player

Not going to talk about Shibboleth/SAML here, but about identity/delegation technology.

There are numerous other technology services evolving in industry - there is at the present time a kind of ecology of these services. For instance, OAuth is somewhat related to OpenID, because of the people involved, but is used to solve delegation-like problems. It's going to be very important - it is the standard Google seems to be adopting, for instance - and it is going to evolve rapidly in the next year, and hybridize with OpenID and with SAML (neither of which has a delegation solution on their own).

InfoCards / Card Space is another one. The metaphor is your wallet full of various cards (VISA, Drivers lic, library card). Kim Cameron's brain child was supposed to be a way of allowing the human to manage multiple identities himself the way we do in the real world. For various reasons it hasn't caught on as ID service but instead seems to be evolving into a kind of authorization or capability card (perhaps that's a better model of what we do in real world too). These "action cards" can also exist on the web too - that is in the cloud. This is very appealing - portable credentials with limited scope.

Mobile platforms - not very visible in the US but we are on the verge of being able to do what a few Asian and EU countries can do, as 3G phones gain market share and new standards support secure transactions better. It's not exactly id as we know it - these are not just big fat smart cards.

We need to study this technology area better and we need to persuade people to support it at some level.

Why are Some VOs so different?

This is as close to an identical twins study as I can imagine doing! Why are such comparable people in such completely different places regarding how we currently provide them access to services? While often mentioned (eg Ruth Pordes at Berkeley in June) it was never more obvious than in the OSG VO part of the workshop.

It is too easy to just dismiss this as some cultural difference - WHAT cultural difference?

Cultural modelers/molders

Something I picked up from James Surowiecki/Wisdom of Crowds - I'd have to hunt to find a good reference but it goes like this: We model our behavior on what others in our group do, and there are influencers in every group, people who are leading the group in some fashion, or early adopters andc. It is likely that in some groups these influencers help us, they show others how to do things and lead the way; in other places these influencers want/need something else and the group models on their rejection.

Privacy

See below. Grids are horrible at privacy and outright reject it. One VO seems to need it.

Anachronism

It may be that there are some organizational life cycle issues - some groups may be at an earlier state. Counterexample: LIGO, which has been around for a long time, and never liked what we do. Never.

How do we deal with differences better? How can we support different organizational work patterns better? Or at all?

We need to understand this sociology or anthropology a lot better. Maybe we need some market research and not guesswork?

Why are we always talking about proxy certificates?

I find it strange that we can't STOP talking about proxy certs. Why are they such a persistent subject? Why do users have even have to know about them? It's something like ... do I have to know what is in my TCP packets and build them? Do I have to know what magic is in different styles in Word? Proxy certificates are a kind of deep infrastructure tool (to me they look like a variation on how to look at PKCS #11 :^) that is sticking up out of its level. (Just for reference ... the proxy cert RFC is June 2004, but I know most of the significant effort was done in 2002.) Sometimes this level of detail is appropriate, but I think we are stuck. And there are other models of delegation to consider.

Privacy and Levels of Assurance

There seems to be a need to discuss this ... but not very much. It's very esoteric, especially the LoA problem, and doesn't seem to meet a program need - regulatory perhaps. How do we deal with this?

Privacy may be different, for medical = related grids, and perhaps for some other less open communities (but see Physics above).   We sure have made it impossible to deal with privacy in Grid identities - I think this is largely driven by LHC but it is also a DOE issue. Making identity end-to-end may also lead to some other undesirable side effects related to Karp and Stiegler's criticisms. Is it worth doing something here?

Persistence/ESnet

What can we say about persistent services, or at least the kinds of things an ESnet or the like can do? What would OSG come to an ESnet-style requirements workshop ~5 mos from now?

Setting up a Virtual Organization

In our group meeting we came back to this discussion - a second day topic. There is a need at some level to provide an easy way for affinity groups and collaborations of various kinds to organize and manage themselves. An interesting metaphor to me is what Google and Yahoo groups do. These services provide a very simple (1 page) initialization screen and simple, straightforward management UI (so it looks to an IT person anyway).

Maybe a more general approach based on an ontology of organizations would be useful; one possible result would be a simple service collecting, organizing, and managing tags (such as some social information services provide).

If this is seen as an important service to offer, some identity questions need to be considered: what kind of identity information needs to be available to the group service; the ontology discussion needs to take into account the tagging of identities and what tags might be needed.