Detailed results from OSG-ESnet Identity Management Survey

Your Name	Name of your community or VO	1. Approximate size of your community	2. Over the next 5 years, is your community growing?
Jeff Porter	ALICE	C: between 100 and 1000	C: will grow some, perhaps twice as many in 5 years
Horst Severini	ATLAS	D: more than 1000	B: will remain about the same as now
John Hover	ATLAS	D: more than 1000	C: will grow some, perhaps twice as many in 5 years
Dennis Box	CDF	C: between 100 and 1000	B: will remain about the same as now
Anand Padmanabhan	CIGI	B: between 10 and 100	D: will probably grow 10X in 5 years
Burt Holzman	CMS	D: more than 1000	C: will grow some, perhaps twice as many in 5 years
Jeffrey Dutton	CompBioGrid	A: less than 10	D: will probably grow 10X in 5 years
Nikolay Kuropatkin	DES	B: between 10 and 100	C: will grow some, perhaps twice as many in 5 years
Horst Severini	DOSAR	B: between 10 and 100	C: will grow some, perhaps twice as many in 5 years
Horst Severini	DZero	C: between 100 and 1000	A: no, it may shrink
joel snow	dzero	B: between 10 and 100	A: no, it may shrink
John McGee	Engage	B: between 10 and 100	C: will grow some, perhaps twice as many in 5 years
Keith Chadwick	fermilab	D: more than 1000	B: will remain about the same as now
Steve Barnet	IceCube	B: between 10 and 100	C: will grow some, perhaps twice as many in 5 years
Kent Blackburn	LIGO	C: between 100 and 1000	C: will grow some, perhaps twice as many in 5 years
Warren Anderson	LIGO	C: between 100 and 1000	C: will grow some, perhaps twice as many in 5 years
Igor Sfiligoi	my group in CMS	B: between 10 and 100	B: will remain about the same as now
Steven Clark	nanoHUB	B: between 10 and 100	D: will probably grow 10X in 5 years
Ruth	OSG	D: more than 1000	D: will probably grow 10X in 5 years
Peter Doherty	SBGrid	B: between 10 and 100	C: will grow some, perhaps twice as many in 5 years
Ian Stokes-Rees	SBGrid	B: between 10 and 100	D: will probably grow 10X in 5 years
Doug Olson	STAR	B: between 10 and 100	May grow some, depends on grid-enabled data analysis

Name of your community or VO	3. Indicate which types of IT resources you use for your science
ALICE	A: OSG grid resources, B: private dedicated non-grid compute and storage resources, D: collaboration content portals like TWiki, Drupal, .., F: group email services (Listserv, HyperNews, Sympa, ...)
ATLAS	A: OSG grid resources, E: social networking sites, such as Facebook, LinkedIn, Yahoo Groups, Google Groups, ..., F: group email services (Listserv, HyperNews, Sympa, ...)
ATLAS	A: OSG grid resources, B: private dedicated non-grid compute and storage resources, C: web portal gateway to batch and/or storage resources, D: collaboration content portals like TWiki, Drupal, .., F: group email services (Listserv, HyperNews, Sympa, ...)
CDF	A: OSG grid resources, B: private dedicated non-grid compute and storage resources, D: collaboration content portals like TWiki, Drupal, .., F: group email services (Listserv, HyperNews, Sympa, ...)
CIGI	A: OSG grid resources, C: web portal gateway to batch and/or storage resources, D: collaboration content portals like TWiki, Drupal, .., Teragrid, NCSA
CMS	A: OSG grid resources, B: private dedicated non-grid compute and storage resources, D: collaboration content portals like TWiki, Drupal, .., F: group email services (Listserv, HyperNews, Sympa, ...)
CompBioGrid	A: OSG grid resources, B: private dedicated non-grid compute and storage resources, D: collaboration content portals like TWiki, Drupal, ..
DES	A: OSG grid resources, B: private dedicated non-grid compute and storage resources, C: web portal gateway to batch and/or storage resources
DOSAR	A: OSG grid resources, B: private dedicated non-grid compute and storage resources, F: group email services (Listserv, HyperNews, Sympa, ...)
DZero	A: OSG grid resources, B: private dedicated non-grid compute and storage resources, F: group email services (Listserv, HyperNews, Sympa, ...)
dzero	A: OSG grid resources, B: private dedicated non-grid compute and storage resources, D: collaboration content portals like TWiki, Drupal, .., F: group email services (Listserv, HyperNews, Sympa, ...), non-OSG grid resources
Engage	A: OSG grid resources, B: private dedicated non-grid compute and storage resources, C: web portal gateway to batch and/or storage resources, D: collaboration content portals like TWiki, Drupal, .., E: social networking sites, such as Facebook, LinkedIn, Yahoo Groups, Google Groups, ..., F: group email services (Listserv, HyperNews, Sympa, ...)
fermilab	A: OSG grid resources, B: private dedicated non-grid compute and storage resources
IceCube	A: OSG grid resources, B: private dedicated non-grid compute and storage resources, C: web portal gateway to batch and/or storage resources, D: collaboration content portals like TWiki, Drupal, .., F: group email services (Listserv, HyperNews, Sympa, ...)
LIGO	A: OSG grid resources, B: private dedicated non-grid compute and storage resources, C: web portal gateway to batch and/or storage resources, D: collaboration content portals like TWiki, Drupal, .., F: group email services (Listserv, HyperNews, Sympa, ...), Non-OSG Grid, LIGO Data Grid
LIGO	A: OSG grid resources, B: private dedicated non-grid compute and storage resources, D: collaboration content portals like TWiki, Drupal, .., F: group email services (Listserv, HyperNews, Sympa, ...), LIGO Data Grid, EVO
my group in CMS	A: OSG grid resources, B: private dedicated non-grid compute and storage resources, C: web portal gateway to batch and/or storage resources, D: collaboration content portals like TWiki, Drupal, .., F: group email services (Listserv, HyperNews, Sympa, ...)
nanoHUB	A: OSG grid resources, B: private dedicated non-grid compute and storage resources, C: web portal gateway to batch and/or storage resources, TeraGrid
OSG	A: OSG grid resources, C: web portal gateway to batch and/or storage resources, D: collaboration content portals like TWiki, Drupal, .., E: social networking sites, such as Facebook, LinkedIn, Yahoo Groups, Google Groups, ..., F: group email services (Listserv, HyperNews, Sympa, ...)
SBGrid	A: OSG grid resources, B: private dedicated non-grid compute and storage resources, C: web portal gateway to batch and/or storage resources, D: collaboration content portals like TWiki, Drupal, ..
SBGrid	A: OSG grid resources, B: private dedicated non-grid compute and storage resources, C: web portal gateway to batch and/or storage resources, D: collaboration content portals like TWiki,

	Drupal, .., E: social networking sites, such as Facebook, LinkedIn, Yahoo Groups, Google Groups, ..., F: group email services (Listserv, HyperNews, Sympa, ...)
STAR	A: OSG grid resources, B: private dedicated non-grid compute and storage resources, D: collaboration content portals like TWiki, Drupal, .., F: group email services (Listserv, HyperNews, Sympa, ...)

Name of your community or VO	4. Indicate which authentication methods you (your community) use for collaborative work related to OSG
ALICE	A: X.509 certificates (grid credentials)
ATLAS	A: X.509 certificates (grid credentials), C: LDAP authenticaiton, G: ssh keys
ATLAS	A: X.509 certificates (grid credentials)
CDF	A: X.509 certificates (grid credentials), B: Kerberos, G: ssh keys
CIGI	A: X.509 certificates (grid credentials), B: Kerberos, F: independent username/password databases
CMS	A: X.509 certificates (grid credentials), B: Kerberos, D: Shibboleth
CompBioGrid	A: X.509 certificates (grid credentials)
DES	A: X.509 certificates (grid credentials), B: Kerberos
DOSAR	A: X.509 certificates (grid credentials), F: independent username/password databases, G: ssh keys
DZero	A: X.509 certificates (grid credentials), B: Kerberos, C: LDAP authenticaiton, G: ssh keys
dzero	A: X.509 certificates (grid credentials), B: Kerberos, C: LDAP authenticaiton, G: ssh keys
Engage	A: X.509 certificates (grid credentials), G: ssh keys
fermilab	A: X.509 certificates (grid credentials), B: Kerberos, C: LDAP authenticaiton
IceCube	A: X.509 certificates (grid credentials), C: LDAP authenticaiton
LIGO	A: X.509 certificates (grid credentials)
LIGO	A: X.509 certificates (grid credentials), B: Kerberos, D: Shibboleth, F: independent username/password databases, G: ssh keys
my group in CMS	A: X.509 certificates (grid credentials), B: Kerberos, F: independent username/password databases, G: ssh keys
nanoHUB	A: X.509 certificates (grid credentials)
OSG	A: X.509 certificates (grid credentials), B: Kerberos, C: LDAP authenticaiton
SBGrid	A: X.509 certificates (grid credentials), F: independent username/password databases, G: ssh keys
SBGrid	A: X.509 certificates (grid credentials), C: LDAP authenticaiton, F: independent username/password databases, G: ssh keys
STAR	A: X.509 certificates (grid credentials), B: Kerberos, F: independent username/password databases, G: ssh keys

Name of your community or VO	5. Importance of using grid credentials to access web portals	6. Issues using the same personal certificate with web browsers, unix shell, email (smime)
ALICE	B: Moderately important	C: problematic for many people they manage it
ATLAS	A: Very important	A: no problems
ATLAS	B: Moderately important	C: problematic for many people they manage it
CDF	C: Not very important	A: no problems
CIGI	A: Very important	B: functional but minor annoyance
CMS	A: Very important	B: functional but minor annoyance
CompBioGrid	D: Does not apply to me	A: no problems
DES	A: Very important	A: no problems
DOSAR	B: Moderately important	A: no problems
DZero	B: Moderately important	A: no problems
dzero	A: Very important	A: no problems
Engage	C: Not very important	C: problematic for many people they manage it
fermilab	A: Very important	D: a lot of trouble and many people can not do it
IceCube	B: Moderately important	A: no problems
LIGO	B: Moderately important	D: a lot of trouble and many people can not do it
LIGO	C: Not very important	D: a lot of trouble and many people can not do it
my group in CMS	A: Very important	B: functional but minor annoyance
nanoHUB	Is there any other choice	personal certifictes only used in web browser for OSG related activites. Trouble but managable
OSG		B: functional but minor annoyance
SBGrid	B: Moderately important	C: problematic for many people they manage it
SBGrid	B: Moderately important	C: problematic for many people they manage it
STAR	C: Not very important	B: functional but minor annoyance

Name of your community or VO	7. Importance of integrating grid credentials with other authentication methods
ALICE	C: Not very important but would be useful
ATLAS	B: Moderately important
ATLAS	B: Moderately important
CDF	D: Unimportant or does not apply to me
CIGI	A: Very important
CMS	D: Unimportant or does not apply to me
CompBioGrid	D: Unimportant or does not apply to me
DES	B: Moderately important
DOSAR	C: Not very important but would be useful
DZero	C: Not very important but would be useful
dzero	A: Very important
Engage	A: Very important
fermilab	A: Very important
IceCube	B: Moderately important
LIGO	A: Very important
LIGO	A: Very important
my group in CMS	C: Not very important but would be useful
nanoHUB	D: Unimportant or does not apply to me
OSG	A: Very important
SBGrid	B: Moderately important
SBGrid	A: Very important
STAR	C: Not very important but would be useful

Name of your community or VO	8. Currently requesting/obtaining a grid certificate and registering with a VOMS server for your VO are two separate procedures. How useful would it be if these were integrated into a single registration process
ALICE	C: not useful or does not apply to me
ATLAS	Would be nice, but how would you do that if you beong to multiple VOs?
ATLAS	B: Would be helpful but not necessary
CDF	B: Would be helpful but not necessary
CIGI	B: Would be helpful but not necessary
CMS	A: Very important
CompBioGrid	B: Would be helpful but not necessary
DES	B: Would be helpful but not necessary
DOSAR	Would be nice, but how would you do that if you beong to multiple VOs?
DZero	Would be nice, but how would you do that if you beong to multiple VOs?
dzero	B: Would be helpful but not necessary
Engage	A: Very important
fermilab	I do not feel that this is a good idea.
IceCube	C: not useful or does not apply to me
LIGO	B: Would be helpful but not necessary
LIGO	B: Would be helpful but not necessary
my group in CMS	B: Would be helpful but not necessary
nanoHUB	B: Would be helpful but not necessary
OSG	A: Very important
SBGrid	A: Very important
SBGrid	A: Very important
STAR	B: Would be helpful but not necessary

Name of your community or VO	9. About the DOEGrids certificate request and issuance process, after a request is submitted and until the certificate is issued
ALICE	mostly functional but with some holes (Safari, missing in action VO reps)
ATLAS	A: no problems
ATLAS	B: functional but annoyning
CDF	B: functional but annoyning
CIGI	B: functional but annoyning
CMS	B: functional but annoyning
CompBioGrid	A: no problems
DES	A: no problems
DOSAR	A: no problems
DZero	A: no problems
dzero	A: no problems
Engage	B: functional but annoyning
fermilab	B: functional but annoyning
IceCube	A: no problems
LIGO	B: functional but annoyning
LIGO	Usually "functional but annoying", sometimes "problematic, takes to long"
my group in CMS	A: no problems
nanoHUB	we don't use DOEGrids certificates
OSG	B: functional but annoyning
SBGrid	A: no problems
SBGrid	B: functional but annoyning
STAR	A: no problems

Name of your community or VO	10. About the DOEGrids CA service, describe significance of problems with CA web site (pki1.doegrids.org)
ALICE	B: functional but minor annoyance
ATLAS	A: no problems
ATLAS	C: Problematic for many people but they mange to use it
CDF	A: no problems
CIGI	B: functional but minor annoyance
CMS	A: no problems
CompBioGrid	A: no problems
DES	A: no problems
DOSAR	A: no problems
DZero	A: no problems
dzero	A: no problems
Engage	D: A lot of trouble, some people can not use it
fermilab	B: functional but minor annoyance
IceCube	A: no problems
LIGO	B: functional but minor annoyance
LIGO	We strongly encourage users to interact via scripts, hence no major problems.
my group in CMS	B: functional but minor annoyance
nanoHUB	we don't use DOEGrids certificates
OSG	
SBGrid	B: functional but minor annoyance
SBGrid	B: functional but minor annoyance
STAR	A: no problems

Name of your community or VO	11. While accessing the DOEGrids CA service, the significance of problems with web browsers
ALICE	functional with holes (safari)
ATLAS	A: no problems
ATLAS	B: functional but minor annoyance
CDF	B: functional but minor annoyance
CIGI	A: no problems
CMS	A: no problems
CompBioGrid	A: no problems
DES	A: no problems
DOSAR	A: no problems
DZero	A: no problems
dzero	A: no problems
Engage	D: a lot of trouble, some people can't make it work
fermilab	Combination of "C" and "D".
IceCube	A: no problems
LIGO	B: functional but minor annoyance
LIGO	We strongly encourage users to interact via scripts, hence no major problems.
my group in CMS	B: functional but minor annoyance
nanoHUB	we don't use DOEGrids certificates
OSG	A: no problems
SBGrid	B: functional but minor annoyance
SBGrid	B: functional but minor annoyance
STAR	B: functional but minor annoyance

Name of your community or VO	12. Rate importance of having the DOEGrids CA trusted by default in web browsers and email
ALICE	B: Very important, many people have trouble installing trusted CA certificates
ATLAS	C: Moderate importance, importing trusted CA certificates is annoying but people manage
ATLAS	A: Extremely important, many people fail to import CA certificate and mark it trusted
CDF	C: Moderate importance, importing trusted CA certificates is annoying but people manage
CIGI	A: Extremely important, many people fail to import CA certificate and mark it trusted
CMS	C: Moderate importance, importing trusted CA certificates is annoying but people manage
CompBioGrid	B: Very important, many people have trouble installing trusted CA certificates
DES	C: Moderate importance, importing trusted CA certificates is annoying but people manage
DOSAR	C: Moderate importance, importing trusted CA certificates is annoying but people manage
DZero	C: Moderate importance, importing trusted CA certificates is annoying but people manage
dzero	C: Moderate importance, importing trusted CA certificates is annoying but people manage
Engage	C: Moderate importance, importing trusted CA certificates is annoying but people manage
fermilab	B: Very important, many people have trouble installing trusted CA certificates
IceCube	B: Very important, many people have trouble installing trusted CA certificates
LIGO	A: Extremely important, many people fail to import CA certificate and mark it trusted
LIGO	B: Very important, many people have trouble installing trusted CA certificates
my group in CMS	A: Extremely important, many people fail to import CA certificate and mark it trusted
nanoHUB	A: Extremely important, many people fail to import CA certificate and mark it trusted
OSG	A: Extremely important, many people fail to import CA certificate and mark it trusted
SBGrid	A: Extremely important, many people fail to import CA certificate and mark it trusted
SBGrid	C: Moderate importance, importing trusted CA certificates is annoying but people manage
STAR	D: Not important, better to improve other aspects of the service

Name of your community or VO	3. The tools for managing many host/service certificates
ALICE	B: Functional but needs improvement
ATLAS	A: Works well, no changes needed
ATLAS	B: Functional but needs improvement
CDF	E: I don't use it
CIGI	A: Works well, no changes needed
CMS	B: Functional but needs improvement
CompBioGrid	A: Works well, no changes needed
DES	A: Works well, no changes needed
DOSAR	A: Works well, no changes needed
DZero	A: Works well, no changes needed
dzero	E: I don't use it
Engage	A: Works well, no changes needed
fermilab	B: Functional but needs improvement
IceCube	I haven't used it yet.
LIGO	C: Some serious deficiencies
LIGO	B: Functional but needs improvement
my group in CMS	A: Works well, no changes needed
nanoHUB	E: I don't use it
OSG	
SBGrid	B: Functional but needs improvement
SBGrid	E: I don't use it
STAR	A: Works well, no changes needed

Name of your community or VO	14. For ID management and credential handling, describe the most valuable features being used in your community
ALICE	Interoperability between credential issuers is critical. As a worldwide organization we require trust between international CAs. I would like to know more about the rules that govern sharing of individual's information between CAs.
ATLAS	From my end, mostly just grid job submission; of course, ATLAS in general also uses VOMS and GUMS management.
ATLAS	For ATLAS, the workload system uses VOMS proxies and MyProxy, so VOMS, VOMRS, and MyProxy are important.
CDF	
CIGI	
CMS	First, grid job submissions (and VOMS extensions to allow role-based authorization controls) and authentication/authorization for file transfers; second, web page authorization (ie for indico at CERN and various CMS-specific services such as siteDB). Lastly, for signing e-mails, although its use is only required in US CMS when ensuring we have a valid chain of trust for the OSG RA to issue new certificates.
CompBioGrid	
DES	
DOSAR	mostly just VOMS server management and grid job submission
DZero	From my end, mostly just grid job submission; of course, DZero in general also uses VOMS and GUMS management.
dzero	x509 certificates and the DOE CA
Engage	Well managed CA
fermilab	Fermilab is very fortunate that our site wide strong authentication system (Kerberos) is able to be used to generate Grid credentials, and there are mechanisms to automatically generate "robot" certificates that can be used in a variety of automatic and automated processes.
IceCube	
LIGO	LIGO is developing a new ID management system which we believe will more closely match the requirements of our user community.
LIGO	Single sign-on, centralized credential management via kerberos relieving both site admins and users from expending effort on IdM and relieving us from supporting that effort, single credential being leveraged for authentication in various IT areas, ability to define attributes meaningful to our VO and decorate credentials with them, ability to delegate management of group attributes to group leaders.
my group in CMS	Credential delegation. VOMS extensions. No need to use per-site passwords. Service/robots credentials.
nanoHUB	
OSG	
SBGrid	
SBGrid	We are not currently using MyProxy, but we were using it and imagine that at some point soon we'll go back to it -- it allows certs (or proxies) to be deposited and then retrieved with just username/password which is sufficient security and in many cases much easier to use. Users get confused with the idea of digital certificates and the need to copy them between browsers and systems (plus associated format conversion). We are using LDAP in some places, and have looked at 389Directory Server (LDAP) more widely -- right now we have users who are identified by: X.509, NIS login, LDAP, htpasswd, and proprietary web portal user DB table. Yuck. From the OSG/Grid side, we are using GUMS, vomsd and VOMSAdmin. We couldn't do our grid work without these, however they aren't always easy to use (see next point). VOMSAdmin and vomsd seem to be reasonable in terms of their functionality.
STAR	It provides authentication to grid resources.

Name of your community or VO	15. For ID management and credential handling, describe the most significant problems encountered in your community
ALICE	the most persistent problems occur mainly because on the infrequency of doing certain operations: renewing a cert, exporting the cert for grid use, moving to a new personal machine (new web & email clients), changing institutions/VOs . None of these operations are difficult but cause user stress because they are both unfamiliar and can interfere with their ability to access needed resources. Simplifying these operations where possible would be useful & making sure there are very clear and complete user documentation is important. For the size of the growing grid user community, I really think that is worth a dedicated effort for documentation of common tasks and pitfalls.
ATLAS	no real problems, as far as I'm aware of
ATLAS	Application, conversion, renewal and use of X509 user certs, and integration of SSL security into VO applications are the most difficult for ATLAS community. Even though the Panda workload system handles job submission, users still need a VOMS proxy to submit to Panda itself.
CDF	
CIGI	
CMS	Most importantly: there's a clear lack of testing and controls when ESnet/DOEGrids makes changes in the certificate format (such as the recent addition of TLS as "critical" extensions). Certificate expiry at one year: a longer lifetime would be nice -- but we also understand the implicit security concern. Establishing the chain of trust via the OSG RA is an annoyance, but with our "certificate team" methodology we have at least distributed the annoyance across 30 institutions. When we do want an extension added to a requested certificate, the command line tools don't currently provide an option to do so (such as the addition of the http server extension in the old days before it was the default).
CompBioGrid	
DES	People sometimes have difficulty to use web interface to VOMRS. Yet I do not think it is a real problem.
DOSAR	no real problems, as far as I'm aware of
DZero	no real problems, as far as I'm aware of
dzero	All collaborators have Kerberos credentials and can get a grid cert from them. This is easier for most members of the VO than getting a DOE cert. Having the Fermi CA recognized is important.
Engage	Web site / browser interaction difficulties when requsting / retrieving certs.
fermilab	1. Changes to the format of the DNs issued by the Fermilab Kerberos Certificate Authority (KCA) that were necessitated by the IGTF accreditation ["/UID=" changed to "/CN=UID:"]. 2. Changes to the CA associated with the DNs issued by the Fermilab Kerberos Certificate Authority (KCA) that were necessitated by the IGTF accreditation [change from "Fermilab KCA" to "Fermilab KCA HSM"]. 3. Fermilab has over 5,000 DNs - managing these changes is a big (thankless) job.
IceCube	
LIGO	Lack of single sign on. Lack of unified authorization across multiple types of resources.
LIGO	User management of X.509 credentials (soon to be eliminated), lack of an academic/scientific CA recognized by default in browsers, secure sharing of secrets (for instance sharing of EVO access passwords).
my group in CMS	CRL expiration... CRL lifetime is way too short, leading to self-inflicted DoS. DOEGrids CA not trusted in the Web browsers. Missing delegation of credentials to the Web server. Risk of compromised delegated credentials due to lack of restrictions during delegation.
nanoHUB	
OSG	
SBGrid	Too many authentication domains, it would be nice for applications, services and more external programs to have native, or simple plugin/API support for x509 identity management
SBGrid	The process of issuing certificates and joining a VO is complicated for most users. Then

	adding in the steps of exporting certs, format conversion, renewal, and the nuances of voms-proxy-init overcome many. A. Streamline the cert-handling process, ideally including the option to issue VO membership requests as part of the initial cert issuance process. Have a clear workflow, show the user where they are in the process and what may be holding up the cert request, and once the cert is retrieved, immediately give them options to request VO membership. A beautiful model would incorporate "pre-authorization" into VOMSAdmin so VO membership could be approved concurrently with CA cert signing/issuance. When the user retrieves their cert they could be told: VO A: pending, VO B: authorized, VO C: denied, etc. A final option may be to enhance MyProxy to have it hold the *true* cert for the user, and to proxy the entire cert request process. The user could then have the option to retrieve the PKCS12 priv/pub cert pair in a file to import to the browser. B. Streamline exported cert handling. Have voms-proxy-init understand PKCS12 files, and just require the user to save it to a particular name and put the file in a particular place -- voms-proxy-init could then do the conversion to usercert.pem and userkey.pem itself, if the files aren't found, or to prompt the user for the PKCS12 file if nothing is found, or give the option to initiate a cert request. Perhaps that should be encapsulated into a wrapper tool "grid-login". C. VO facilities are weak. Some kind of hierarchical arrangement would be nice, so authorization could be granted to users at a given level in a tree (implying all lower levels), and for operation ACLs to require at least a particular level of authority (implying all higher levels are also acceptable). We would like to see support for user-driven VO-membership controls. This would fit in to a hierarchical model where a user at a particular level could control access to anyone at a lower level (or even create/define lower levels). The idea is to enable users to establish their own "dynamic VOs" that represent a short lived collaboration, and then to have user-group access controls associated with the members of this "dynamic VO" (or sub VO, or whatever name you want to give it). D. Better programmatic tools for working with idM and credentials. E. Some standardized roles or ACs would allow sites to manage capabilities such as "a user from any VO with the role 'software manager' can place files in $OSG_APP".
STAR	Initial registration with the VO is troublesome but happens only once. There is a bit of a learning curve for new people to understand their grid credentials but once they learn the is not much trouble.

Name of your community or VO	16. Briefly describe the types of privileges used in your community and how they are managed
ALICE	In ALICE, Grid administrators have roles which allow them to install software and manage job submission. General users are allowed to submit jobs on all compliant resources and access all ALICE data on the grid infrastructure. Roles are managed through VOMS.
ATLAS	For me, just grid client submission with a grid or voms proxy; I'm not too familiar with the software installation or production running parts of ATLAS..
ATLAS	Briefly, ATLAS has a production role, with full privileges, a software role for VO software installation. Any other VO users get low privileges. Since the Panda workload system handles most analysis, and DQ2 handles most data mangagement, individual users rarely interact directly with grid components.
CDF	
CIGI	
CMS	We manage most of our privileges through VOMS roles limited to small numbers of users each. We have a "production" VOMS role for running large-scale production on our dedicated resources. We have a software role ("cmssoft") for performing software installations. We have "t1access" VOMS roles for non-production use of our 7 Tier 1 facilities. We have different VOMS groups corresponding to analyses that are not yet in wide use, but conceivably could be used to differentiate priorities based on physics as well as separating out storage targeted towards particular analyses. Finally, we have a newly implemented "priorityuser" role that gives priority access to 25% of Tier 2s compute resources as well as special write access within a storage element.
CompBioGrid	At this moment, our site is very simple with no sophisticated roles. Anything requiring an administrator type of a role is done by site admins.
DES	For now all users got the same level privileges managed through VOMS. In some cases we restrict external users to read only access to local data servers.
DOSAR	DOSAR currently doesn't use roles, so we're happy with both grid-mapfile and GUMS access.
DZero	For me, just grid client submission with a grid or voms proxy; I'm not too familiar with the software installation and production running parts of DZero.
dzero	To my knowledge roles are not used.
Engage	using groups managed through VOMS to classify our user types for reporting purposes.
fermilab	1. Grid administrator access to systems that offer fundimental Grid services (VOMS, GUMS, SAZ, etc.) is controlled through the use of Kerberos based credentials. 2. Grid users are mapped using the OSG GUMS software, the precise privileges granted to the various roles is subject to negotiation with the particular VO and Fermilab. This is largely based on the GUMS template distributed by the OSG in the VO package.
IceCube	
LIGO	All users on the LIGO Data Grid are granted shell accounts which are accessed with their DOE Grids certs. There is in general no user distinction other than those few with superuser privileges on a resource.
LIGO	There are many different privilege schemes: - gsissh shell access with sudo for administrators on LDG - authorization to management functions via native delegation options in grouper - equal access for all users via voms on OSG - etc
my group in CMS	We mostly use a single group/role. CMS operations use special roles for software installation, but most users use just a single group/role.
nanoHUB	A single community certificate is used for all end users. All end users are currently

	treated equally. A different certificate is used for monitoring sites.
OSG	
SBGrid	Currently the privileges are flat, no unique priorities for users. Any administrative actions happen outside grid identity management (ie root ssh access)
SBGrid	Users can control read/write access on their submitted jobs and the resulting data via a web-portal i/f. Some of the access control is implemented via the web framework, some via GACL (mod_gridsite) on the file system exposed by httpd (apache), and some via .htaccess/.htpasswd. We have software managers who install and configure software on sites, placing it into $OSG_APP/sbgrid, and also stage static/persistent job data into $OSG_DATA/sbgrid. This is done on a policy basis, rather than controlled by credentials or software. We have some users that submit jobs directly from an OSG client and use their own DoE X.509 cert associated with one of the two VOs we manage: SBGrid or NEBioGrid. We have some users that submit jobs via a web portal. The jobs use a shared portal certificate to run on a particular site. Our various privilege levels are: super user staff portal user (portal based job submission using portal shared cert) software manager grid user (personal cert with VO-affiliation) shared access (anonymous user who knows a shared access password) group access (GACL DN list controlled access to a resource based on defined set of DNs) Access control targets: file access (read/write/list -- we'd like to add append, but don't have the underlying facility for this yet) meta-data access task/job creation/submission portal access operation access (e.g. reset, deleted, restart, status) User identity comes from: ssh keys NIS LDAP web framework (custom user table) X.509 .htpasswd
STAR	There are two privilege levels, production user and regular user. Mapping to these privileges is handled manually at the sites belonging to the VO (STAR). On other resources only a single privilege level is used. VOMS is not used for attributes, just membership.