Grid Security

Grid security is a crucial component

- Need for secure communication
  - Authenticated (verify entities are who they claim to be -> use certificates and CAs)
  - Confidential - only invited to understand conversation (use encryption)

  between grid elements
- Need to support security across organizational boundaries
  - No centrally managed security system
- Need to support “single sign-on” for users of grid
  - Delegation of credentials for computations that involve multiple resources and/or sites
  - allowing or denying access to services based on policies (authorization)

Identity & Authentication

- Each entity should have an identity
- Authenticate: Establish identity
  - Is the entity who he claims he is ?
  - Examples:
    - Driving License
    - Username/password
- Stops masquerading imposters

Authorization

- Establishing rights
- What can a certain identity do ?

Examples:

- Are you allowed to be on this flight ?
  - Passenger ?
  - Pilot ?
- Unix read/write/execute permissions

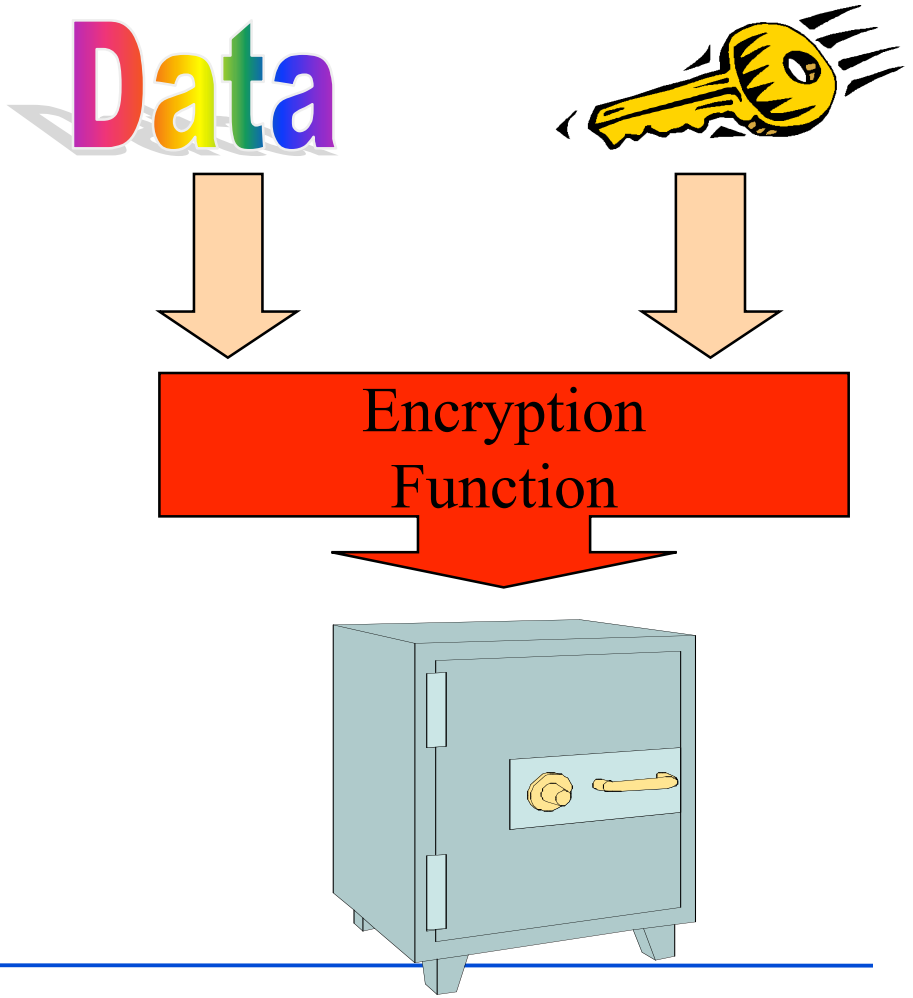
- Must authenticate first

Single Sign-on

- Important for complex applications that need to use Grid resources
  - Enables easy coordination of varied resources
  - Enables automation of process
  - Allows remote processes and resources to act on user's behalf
  - Authentication and Delegation

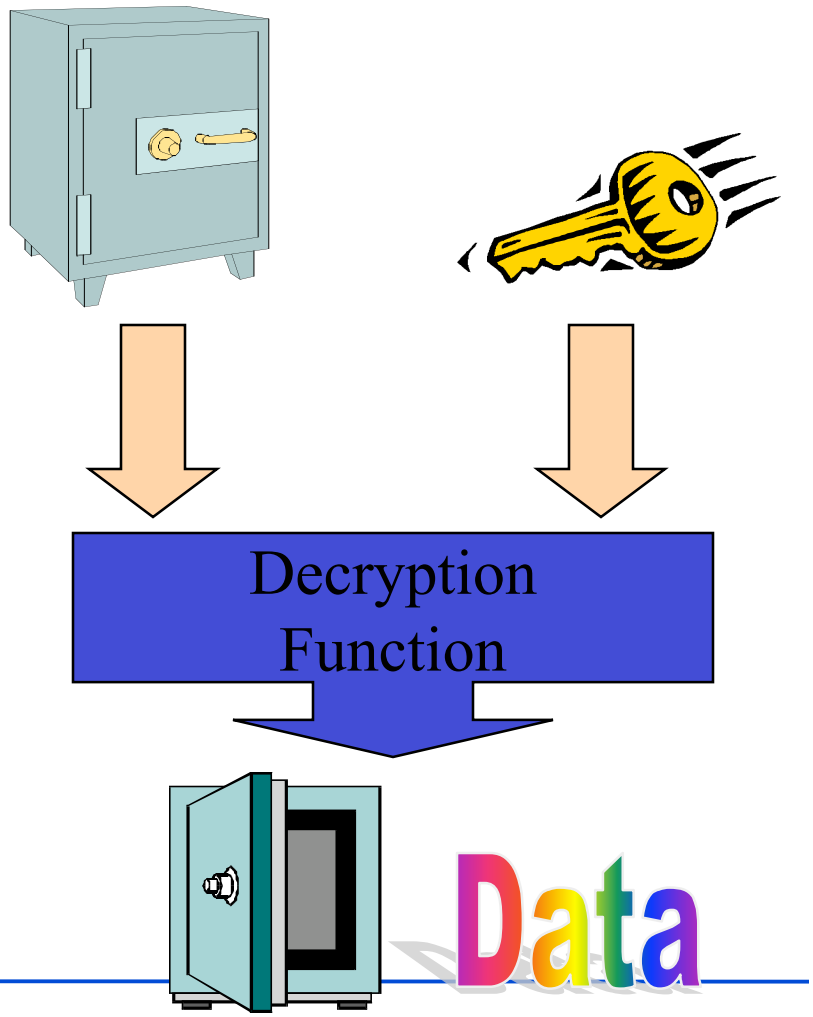
Encryption

- Encryption is the process of taking some data and a key and feeding it into a function and getting encrypted data out
- Encrypted data is, in principal, unreadable unless decrypted



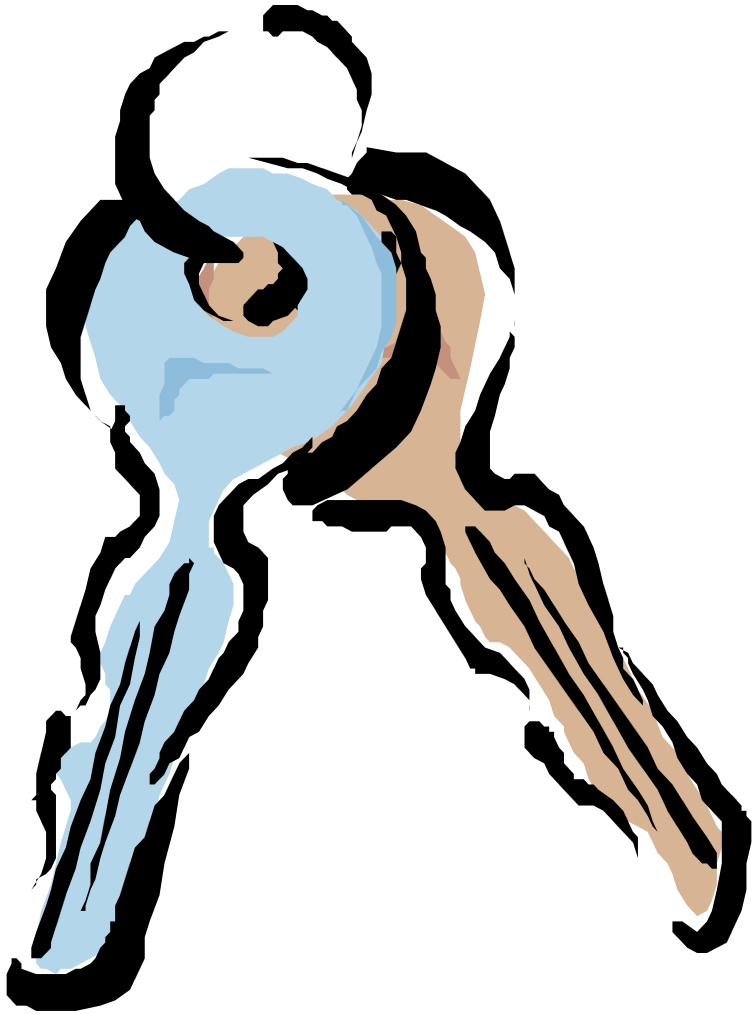
Decryption

- Decryption is the process of taking encrypted data and a key and feeding it into a function and getting out the original data
  - Encryption and decryption functions are linked



Asymmetric Encryption

- Encryption and decryption functions that use a key pair are called asymmetric
  - Keys are mathematically linked



Public and Private Keys

- With asymmetric encryption each user can be assigned a key pair:

  a **private** and a **public** key

Private key is known only to owner

Public key is given away to the world

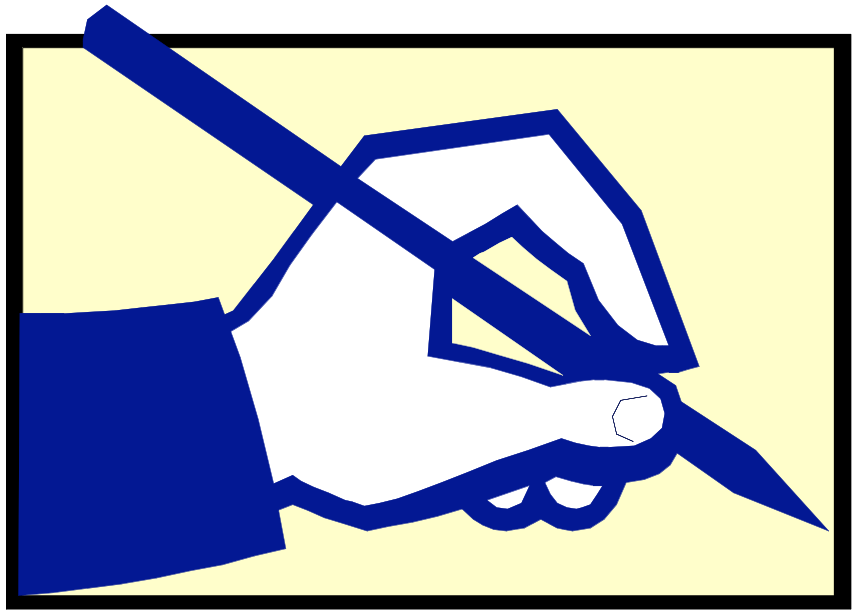
- Encrypt with public key, can decrypt with only private key
- Message Privacy

Public Key Infrastructure (PKI)

- PKI allows you to know that a given public key belongs to a given user
- PKI builds off of asymmetric encryption:
  - Each entity has two keys: public and private
  - The private key is known only to the entity
- GSI is based on PKI
- The public key is given to the world encapsulated in a X.509 certificate

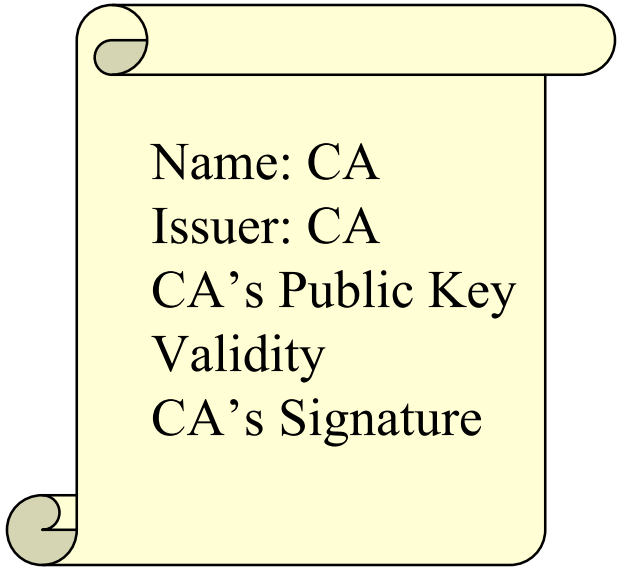
Digital Signatures

- Digital signatures allow the world to
  - determine if the data has been tampered
  - verify who created a chunk of data
- Sign with private key, verify with public key
- Message Integrity



Certification Authorities (CAs)

- A Certification Authority is an entity that exists only to sign user certificates
- The CA signs its own certificate which is distributed in a trusted manner
- Verify CA certificate, then verify issued certificate



Certificates

- Central concept in GSI authentication
- Every user, resource and service on Grid is identified via a certificate
- Contains:
  - **Subject name (identifies entity)**
  - **Corresponding public key**
  - **Identity of the CA that has signed the cert (***to certify that the public key and the identity both belong to the subject***)**
  - **The digital signature of the CA**
- GSI certs are encoded in a X509 certificate format

Many CA's exist

- Indeed, many CA providers exist
- ESNet:
  - **DOEGrids (doegrids.org)**
  - ESNet Root
  - NorduGrid
  - Russian Data Intensive Grid

Globus Security:

- GSI - is a set of tools, libraries and protocols used in Globus to allow **users** and **applications** to securely access resources.
- Based on PKI
- Uses Secure Socket Layer for authentication and message protection
  - Encryption
  - Signature
- Adds features needed for Single-Sign On
  - Proxy Credentials
  - Delegation

Authorization - Gridmap

- **Gridmap** is a list of mappings from allowed DNs to user name

  "/C=US/O=Globus/O=ANL/OU=MCS/CN=Ben Clifford" benc
  "/C=US/O=Globus/O=ANL/OU=MCS/CN=MikeWilde" wilde
  (in /etc/grid-security/grid-mapfile directory)

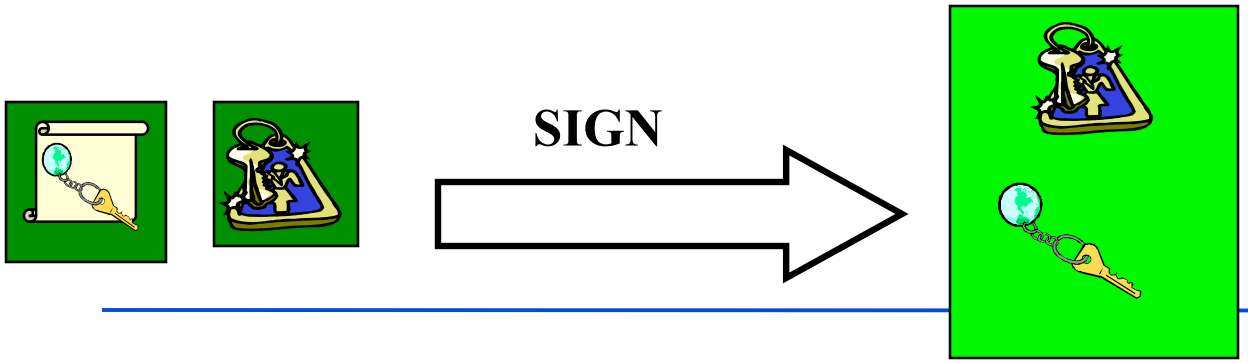
- Controlled by administrator
- Open read access

GSI: Credentials

- In the GSI system each user has a set of credentials they use to prove their identity on the grid
  - Consists of a X509 certificate and private key
- **Long-term** private key is kept encrypted with a pass phrase
  - Good for security, inconvenient for repeated usage
  - Do not lose this phrase !

GSI: Proxy Credentials

- Proxy credentials are ***short-lived*** credentials created by user
  - Proxy is signed by certificate private key
- Short term binding of user's identity to alternate private key
- Same effective identity as certificate



GSI: Proxy Credentials

- Stored unencrypted for easy repeated access
- Chain of trust
  - Trust CA -> Trust User Certificate -> Trust Proxy
- Key aspects:
  - Generate proxies with ***short*** lifetime Set appropriate permissions on proxy file
  - Destroy when done

Grid Security - in practice - steps:

- Get certificate from relevant CA
  - DOEGrids in our case
- Request to be authorized for resources
  - Meaning you will be added to the OSGEDU VOMS
- Generate proxy as needed
  - Using grid-proxy-init
- Run clients
  - Authenticate
  - Authorize
  - Delegate as required

Numerous resources, different CAs, numerous credentials

National Grid Cyberinfrastructure

Grid Resources in the US

The OSG

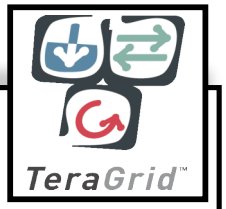
Origins:

- National Grid (iVDGL, GriPhyN, PPDG) and LHC Software & Computing Projects

Current Compute Resources:

- 61 Open Science Grid sites
- Connected via Inet2, NLR.... from 10 Gbps – 622 Mbps
- Compute & Storage Elements
- All are Linux clusters
- Most are shared
  - Campus grids
  - Local non-grid users
- More than 10,000 CPUs
  - A lot of opportunistic usage
  - Total computing capacity difficult to estimate
  - Same with Storage

The TeraGrid



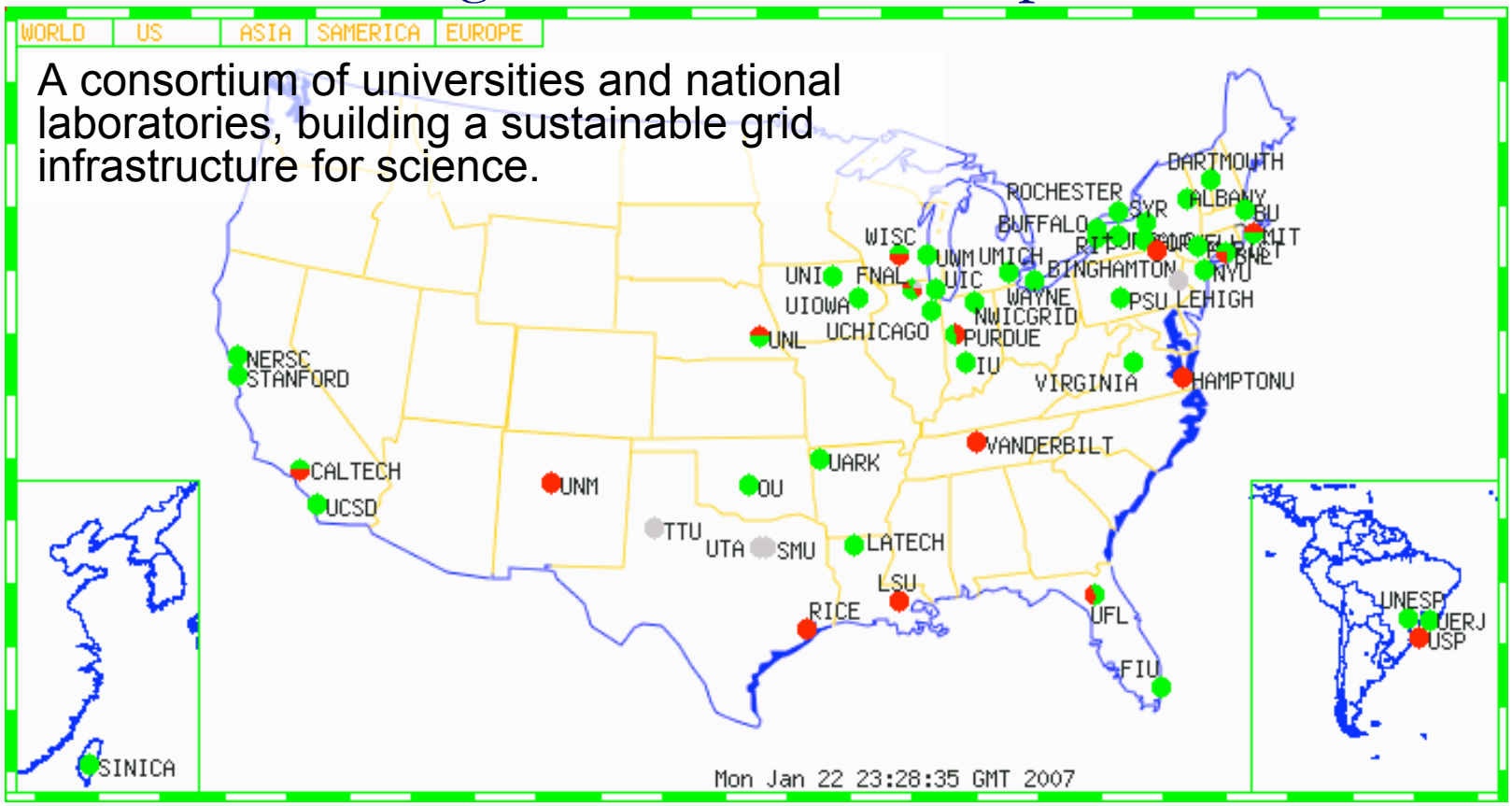
Origins:

- National Super Computing Centers, funded by the National Science Foundation

Current Compute Resources:

- 14 TeraGrid sites
- Connected via dedicated multi-Gbps links
- Mix of Architectures
  - ia64, ia32 LINUX
  - Cray XT3
  - Alpha: True 64
  - SGI SMPs
- Resources are dedicated but
  - Grid users share with local users
  - 1000s of CPUs, > 40 TeraFlops
- 100s of TeraBytes

Open Science Grid (OSG) provides shared computing resources, benefiting a broad set of disciplines

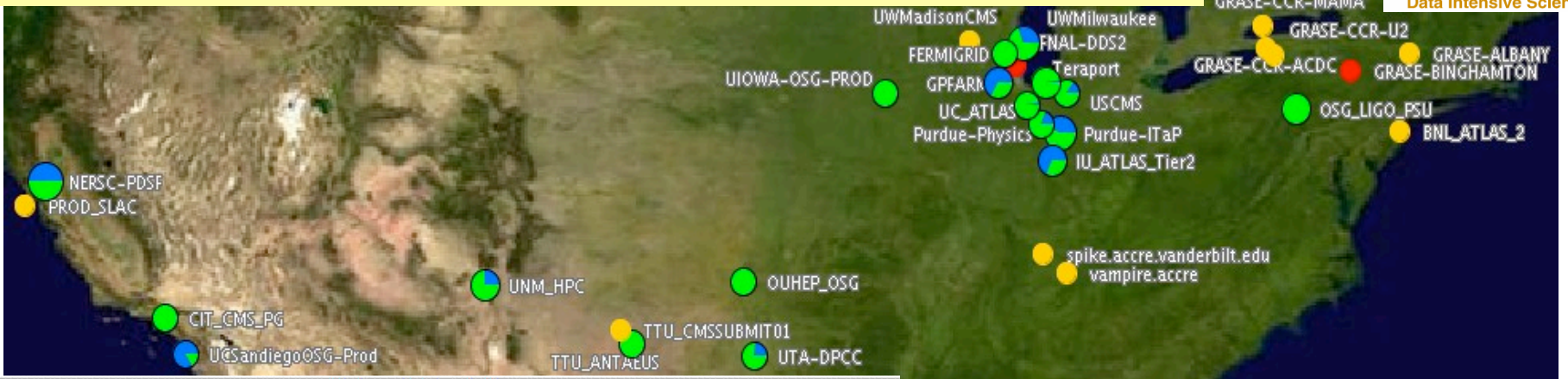


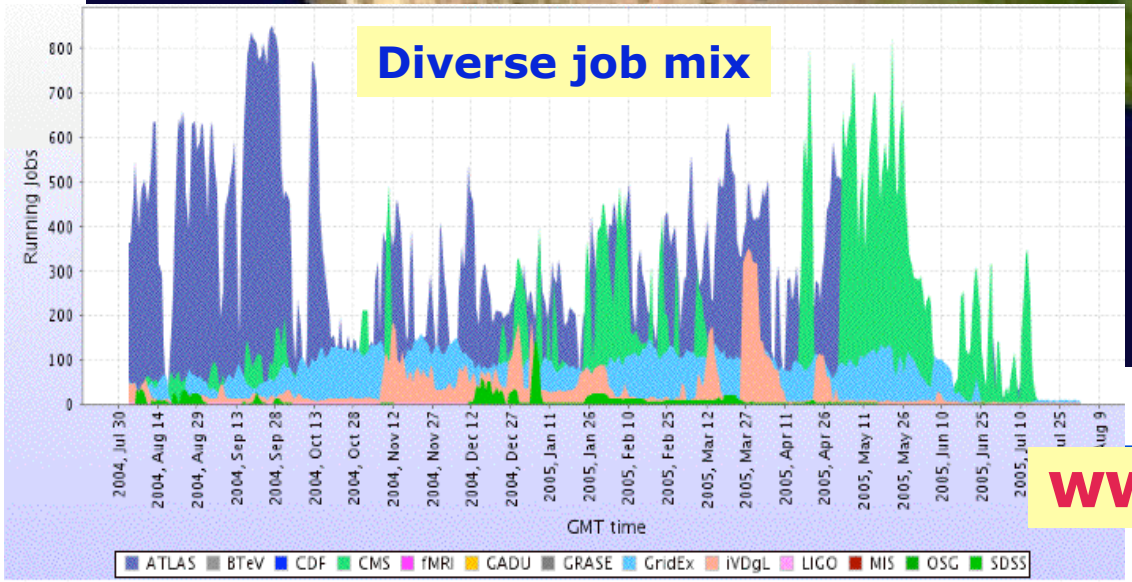
- OSG incorporates advanced networking and focuses on general services, operations, end-to-end performance
- Composed of a large number (>50 and growing) of shared computing facilities, or "sites"

http://www.opensciencegrid.org/

Open Science Grid

- 70 sites (25,000 CPUs) & growing
- 400 to >1000 concurrent jobs
- Many applications + CS experiments; includes long-running production operations
- Up since October 2003;

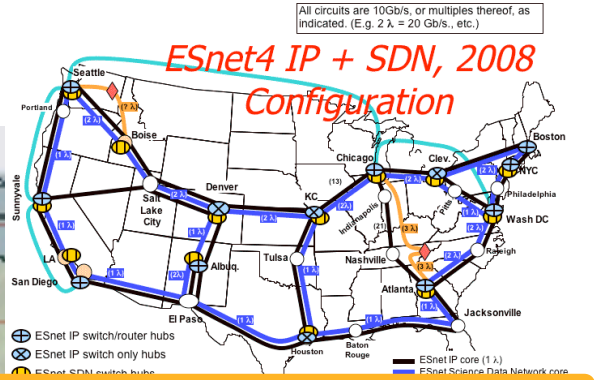




www.opensciencegrid.org

OSG Snapshot

96 Resources across
production & integration infrastructures



Using production & research networks

Sustaining through OSG submissions:
3,000-4,000 simultaneous jobs .
~10K jobs/day
~50K CPUhours/day.
Peak test jobs of 15K a day.

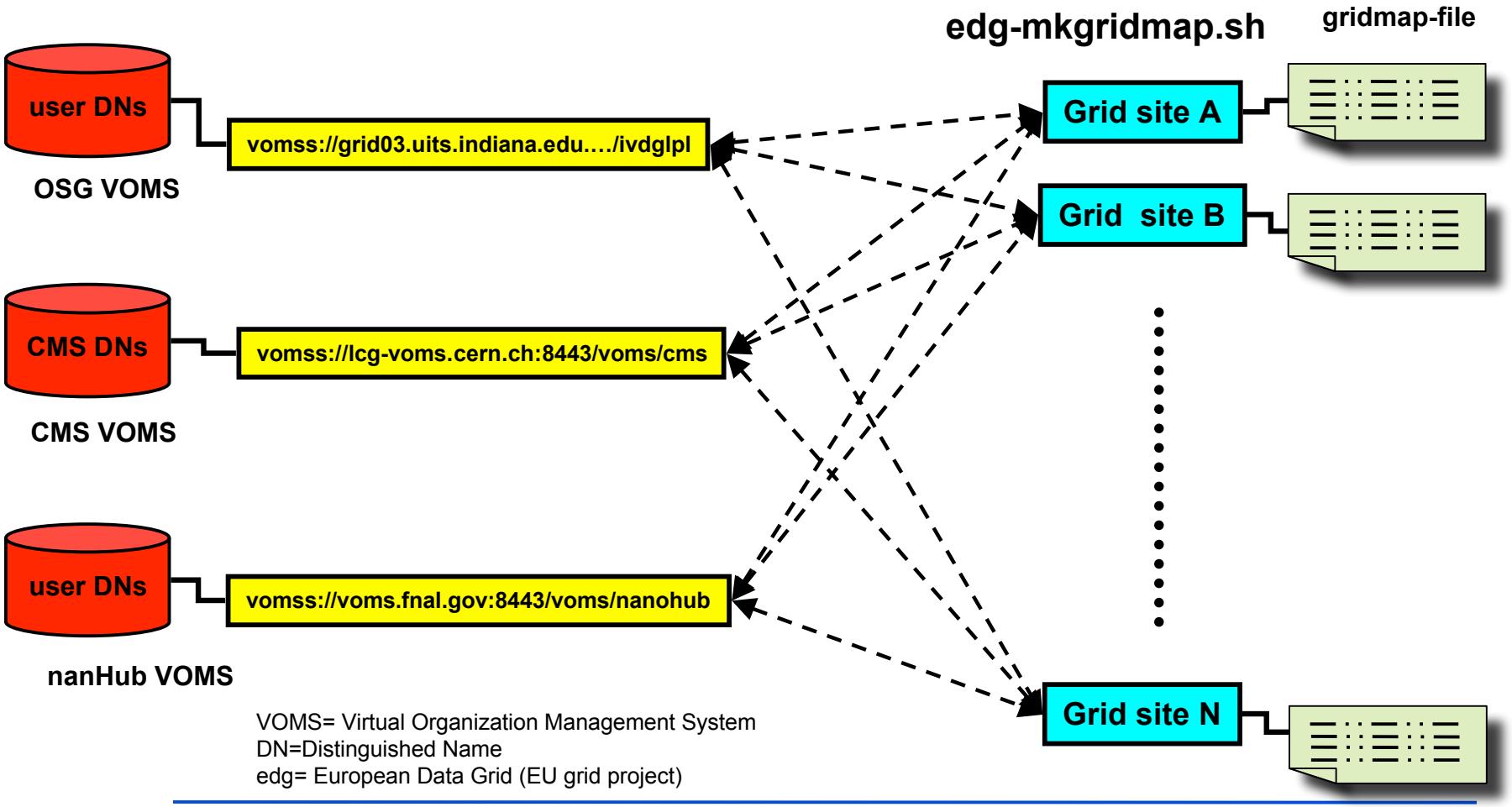
~20,000 CPUs (from 30 to 4000)
~6 PB Tapes
~4 PB Shared Disk

Snapshot of Jobs on OSGs

Farm	Last value	Min	Avg	Max
ATLAS	259	0	338.8	1516
CDF	1278	0	336.6	2086
CMS	579	0	439	3733
DES	39	0	0.385	40
DOSAR	25	0	9.93	192
FERMILAB	4	0	21.38	192
GADU	0	0	23.84	730
GLOW	0	0	35.44	541
GRIDEX	29	0	20.36	268
GROW	41	0	1.434	111
IVDGL	0	0	0.852	73
KTEV	35	0	15.52	260
LIGO	13	0	2.539	88
MINIBOONE	1053	0	128.7	1254
MIPP	2	0	15.32	206
MIS	0	0	0.269	20
NANOHUB	99	0	26.83	187
OPS	2	0	0.017	3
OSG	0	0	0.226	11
SDSS	33	0	3.941	199
STAR	38	0	12.77	150
Total	**3529**		**1434**	

20 Virtual Organizations +6 operations
Includes 25% non-physics.

VOMS



VOMS= Virtual Organization Management System
DN=Distinguished Name
edg= European Data Grid (EU grid project)

To efficiently use a Grid, you must **locate and monitor its resources.**

- Check the availability of different grid sites
- Discover different grid services
- Check the status of “jobs”
- Make better scheduling decisions with information maintained on the “health” of sites

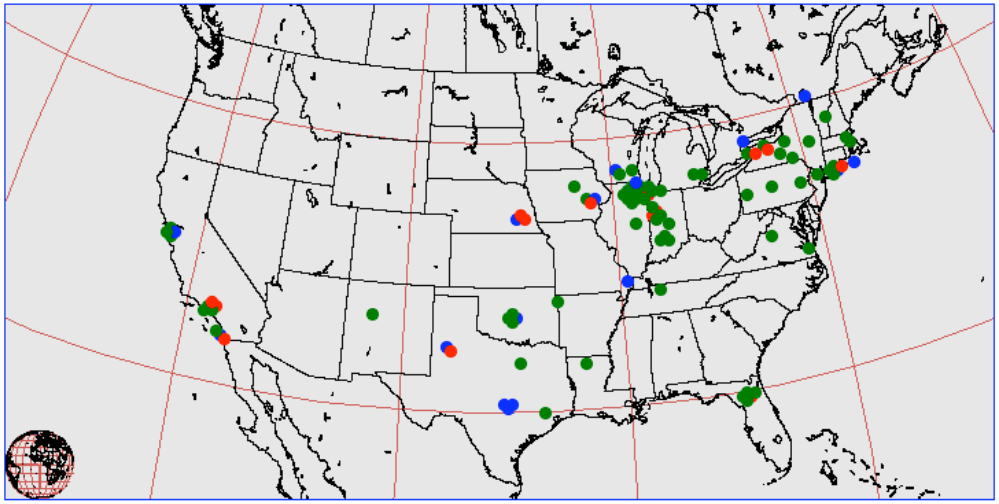
OSG - VORS (VO Resource Locator)

http://vors.grid.iu.edu/cgi-bin/index.cgi?grid=0&VO=0&res=0&region=1

Virtual Organization Resource Selector

All	OSG	TeraGrid	EGEE	OSG-ITB

Open Science Grid



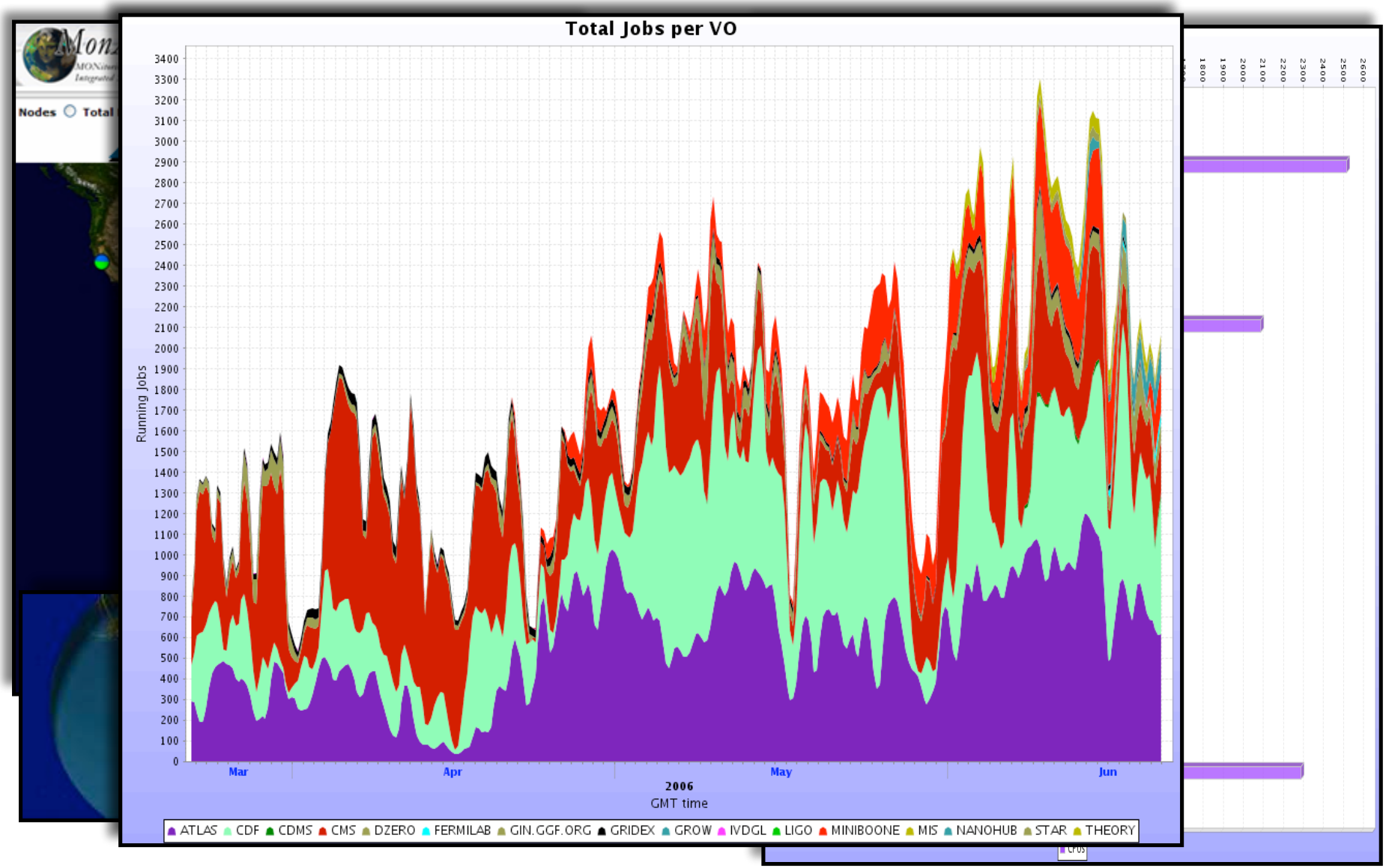
Virtual Organization Selection

All	CDF	CMS	CompBioGri	DES	DOSAR	DZero	Engage	Fermilab	fMRI	GADU
	geant4	GLOW	GPN	GRASE	GridChem	GridEx	GROW	i2u2	iVDGL	LIGO
mariachi	MIS	nanoHUB	NWICG	Ops	OSG	OSGEDU	SDSS	STAR	USATLAS	

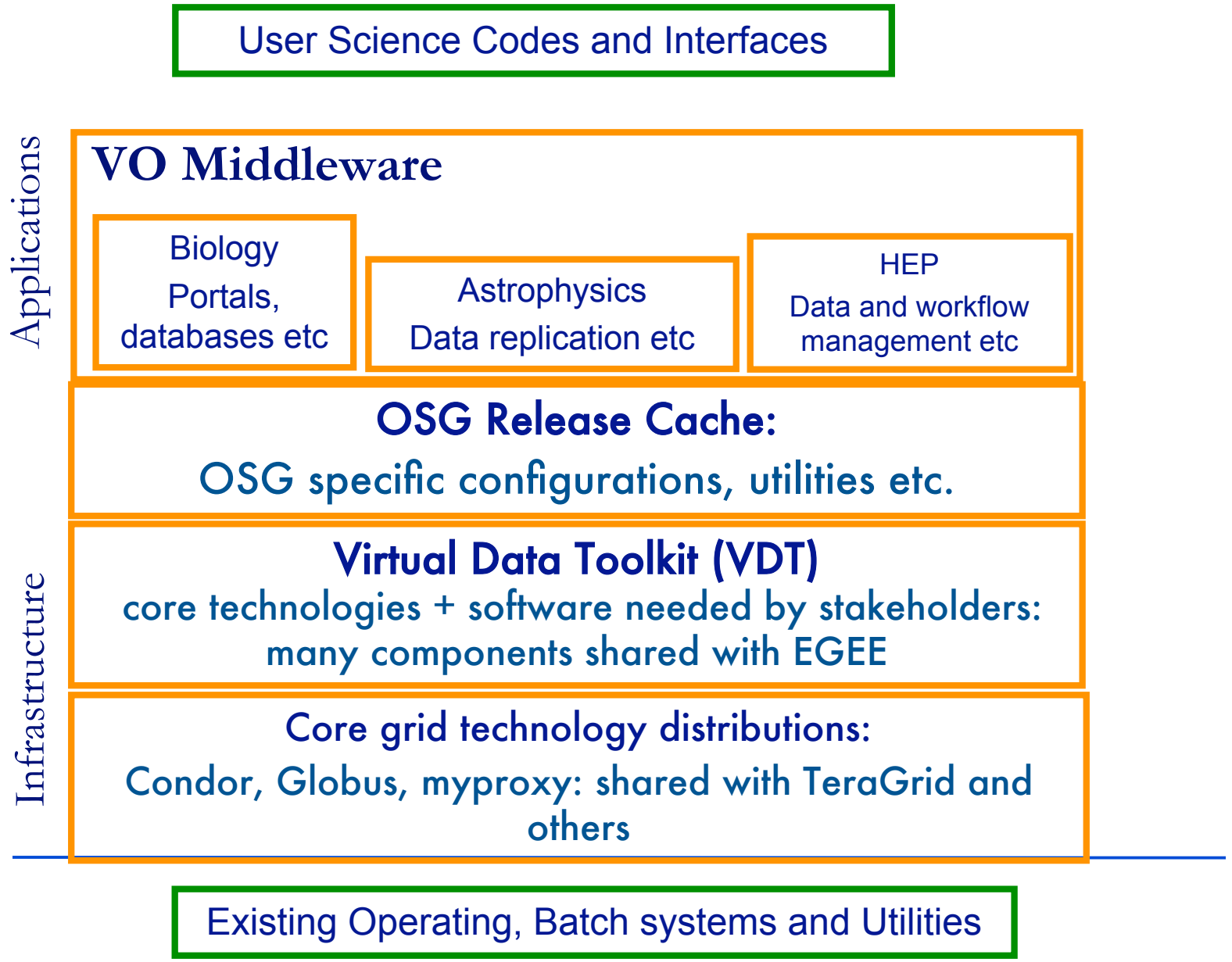
Resources

Name	Gatekeeper	Type	Grid	Status	Last Test Date
BNL_ATLAS_1	gridgk01.racf.bnl.gov:2119	compute	OSG	PASS	2006-12-08 14:57:13
BNL_ATLAS_2	gridgk02.racf.bnl.gov:2119	compute	OSG	PASS	2006-12-08 14:58:43
BU_ATLAS_Tier2	atlas.bu.edu:2119	compute	OSG	PASS	2006-12-08 15:00:44

OSG - Monitoring - MonALISA



OSG Middleware



What's included in VDT ?

- GRAM: Allow job submissions
- GridFTP: Allow file transfers
- CEMon/GIP: Publish site information
- Some authorization mechanism
  - grid-mapfile: file that lists authorized users
  - GUMS: service that maps users
- other pieces of software

TeraGrid provides vast resources via a number of huge computing facilities.

world's largest, most comprehensive distributed cyberinfrastructure for open scientific research (750 teraflops of computing capability and more than 30 petabytes of storage)

The TeraGrid

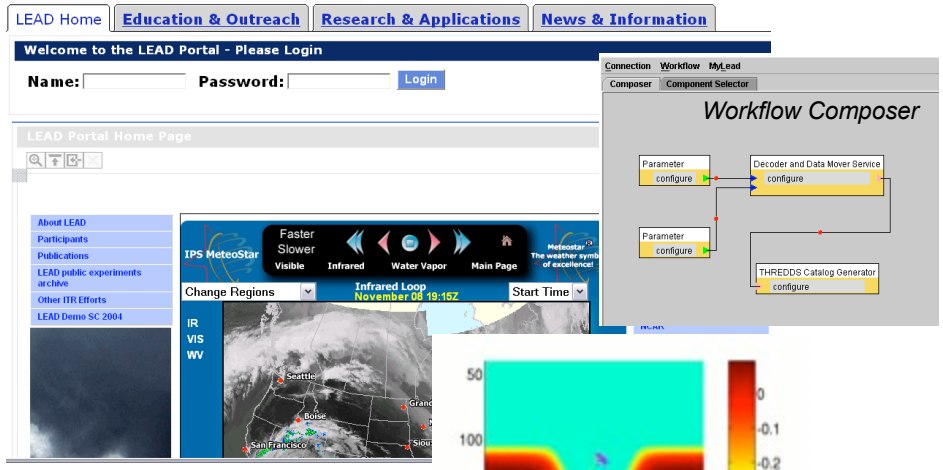
- open scientific discovery infrastructure combining leadership class resources at 11 partner sites to create an integrated, persistent computational resource

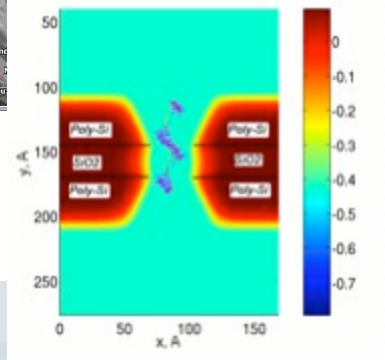
- 750 teraflops of computing capability and more than 30 petabytes of online and archival data storage

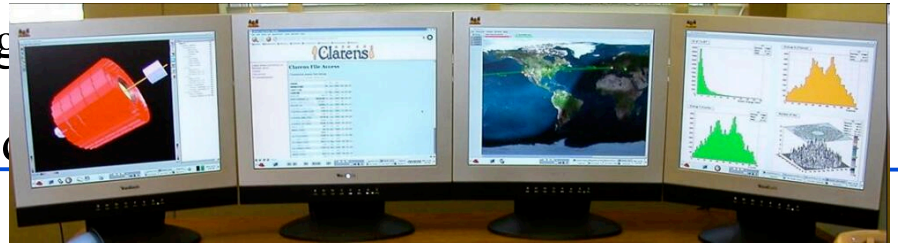
- Resource Providers:
  - Currently NCSA, SDSC, PSC, Indiana, Purdue, ORNL, TACC, UC/ANL
  - Systems (resources, services) support, user support
  - Provide access to resources via policies, software, and mechanisms coordinated by and provided through the GIG (coordinated through the Grid Infrastructure Group (GIG) at the University of Chicago)

Science Gateways
A new initiative for the TeraGrid

- Increasing investment by communities in their own cyberinfrastructure, but heterogeneous:
  - Resources
  - Users – from expert to K-12
  - Software stacks, policies
- Science Gateways
  - Provide "TeraGrid Inside" capabilities
  - Leverage community investment
- Three common forms:
  - Web-based Portals
  - Application programs running on users' machines but accessing services in TeraGrid
  - Coordinated access points enabling users to move seamlessly between TeraGrid







For More Info

- Open Science Grid
  - http://www.opensciencegrid.org
- TeraGrid
  - http://www.teragrid.org

Conclusion: Why Grids?

- New approaches to inquiry based on
  - Deep analysis of huge quantities of data
  - Interdisciplinary collaboration
  - Large-scale simulation and analysis
  - Smart instrumentation
  - ***Dynamically assemble the resources to tackle a new scale of problem***
- Enabled by access to resources & services without regard for location & other barriers

Grids:
Because Science needs community …

- Teams organized around common goals
  - People, resource, software, data, instruments…
- With diverse membership & capabilities
  - Expertise in multiple areas required
- And geographic and political distribution
  - No location/organization possesses all required skills and resources
- Must adapt as a function of the situation
  - Adjust membership, reallocate responsibilities, renegotiate resources

Acknowledgments:

Presentation based on different OSG speaker notes (globus, condor, swift, GSI teams).