Simplifying FusionGrid Security

Presented by
Justin Burruss

CLADE 2005

Research Triangle Park, NC
July 24, 2005

burruss@fusion.gat.com
http://web.gat.com/~burruss/

Acknowledgements

- **U. S. Department of Energy**
  - OFES & OASCR (SciDAC)
- **DIII-D National Fusion Facility**
  - Operated by General Atomics
- **FusionGrid collaborators**
  - MIT, PPPL, LBL, ANL, Utah CS, Princeton CS

Outline

- **Background**
  - What is fusion?
  - What is FusionGrid?
- **Problem**
  - Initial FusionGrid security did not meet needs
- **Solution**
  - Credential management
  - Authorization management
- **Outcome**
- **Conclusion**

Presentation Key Points

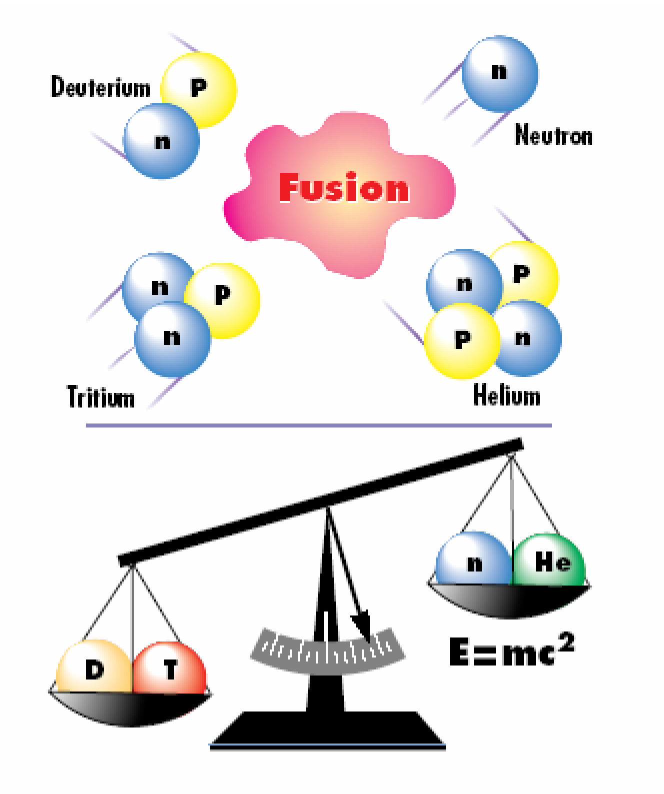
- **FusionGrid required security across administrative domains that**
  - met site security needs
  - met resource owner needs
  - did not stifle developer innovation
  - was usable by mere mortals

- **FusionGrid developers addressed these needs by**
  - replacing self-management of credentials with MyProxy
  - creating a grid-wide authorization management system (ROAM)

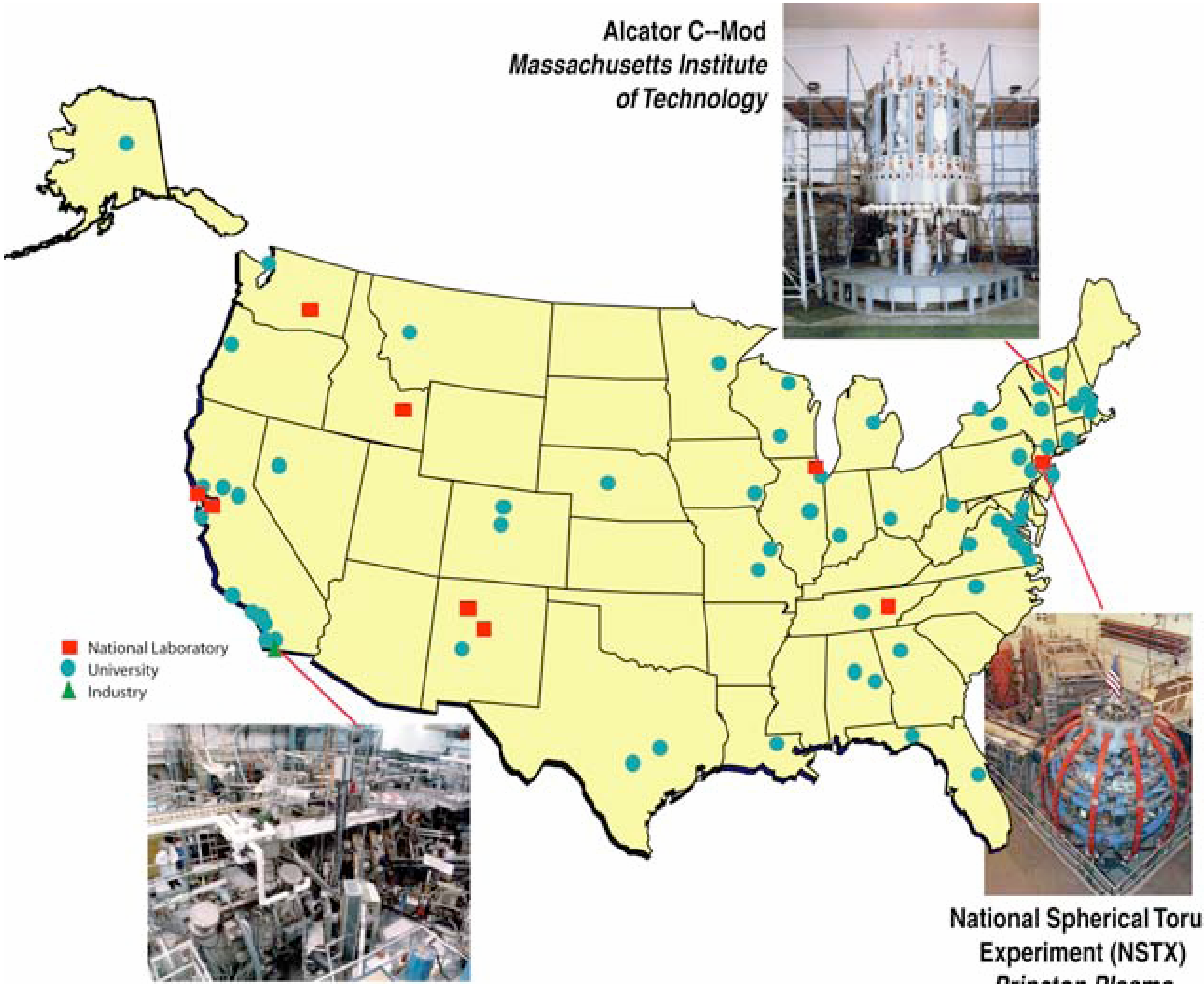
- **Users, admins, and developers responded positively**

Fusion science seeks an environmentally & economically attractive power plant

- **Fusion is when you combine two atoms into one atom**
- **Energy is released from this fusion reaction**
- **An attractive power source**
  - Abundant fuel available to all nations
  - Environmentally friendly
  - No proliferation risk
  - Can’t blow up/melt down
  - Not subject to weather/seasonal issues
  - Concentrated relative to wind/solar



Fusion research takes place across the U. S.

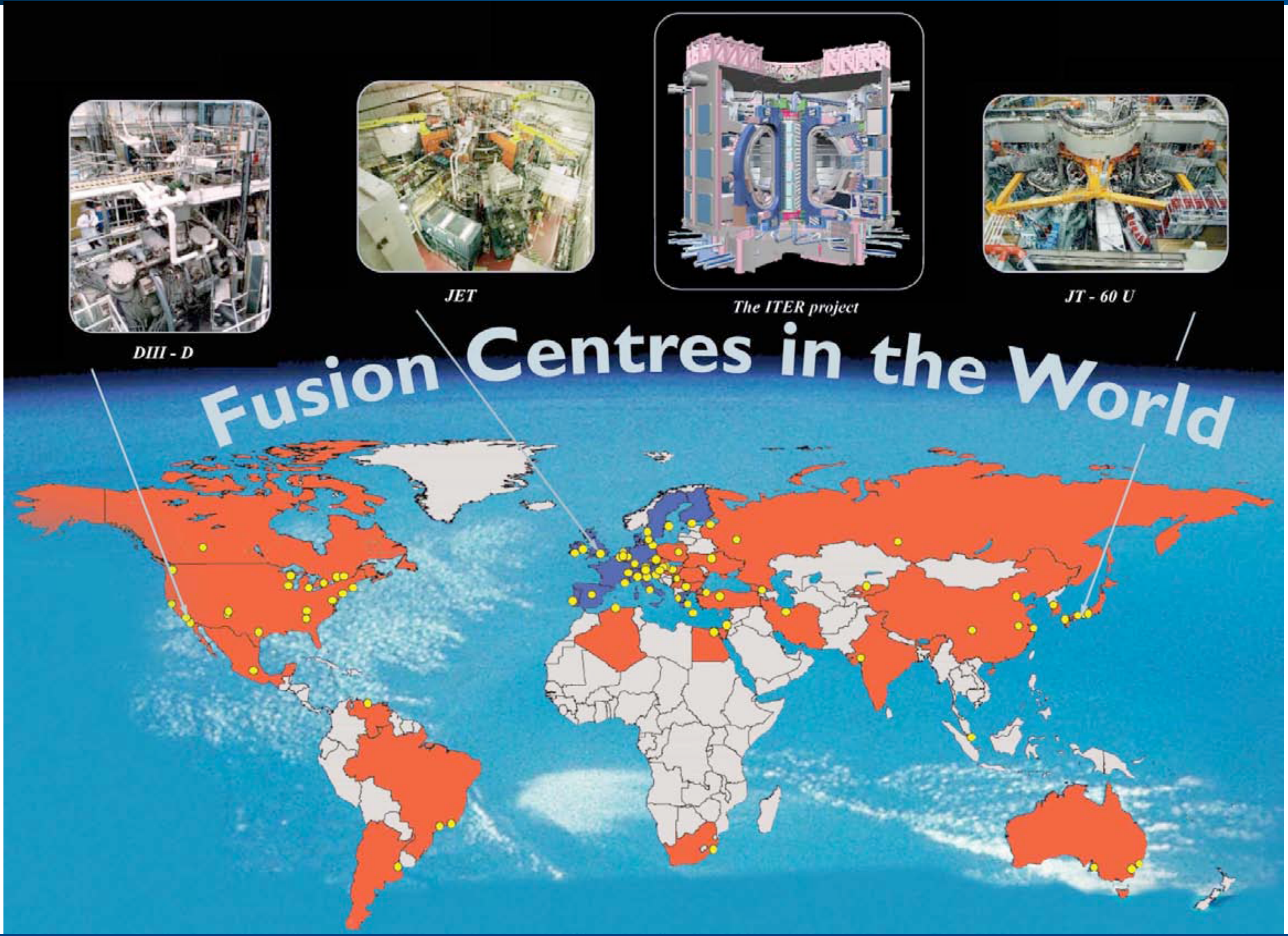


Alcator C--Mod
Massachusetts Institute of Technology

DIII–D General Atomics
San Diego, Ca

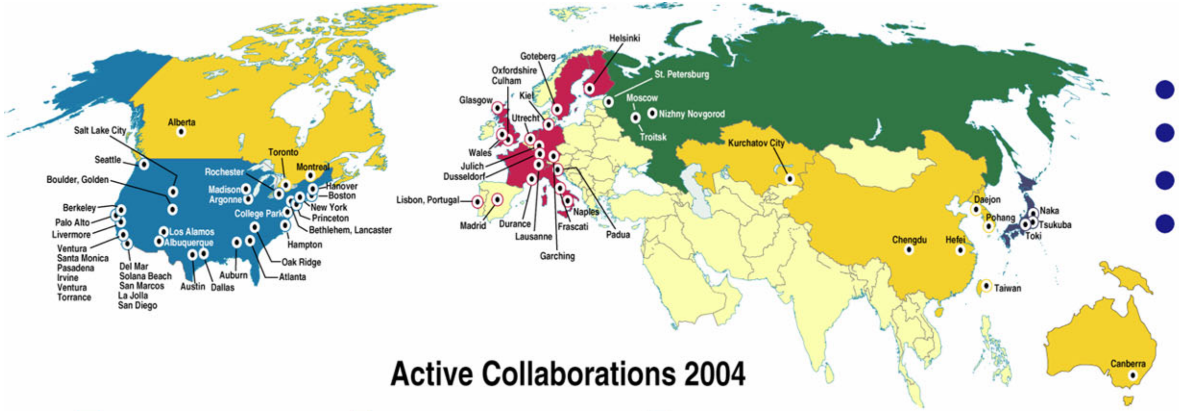
National Spherical Torus Experiment (NSTX)
Princton Plasma Physics Laboratory

Fusion research takes place worldwide



FusionGRID
www.fusiongrid.org

Fusion research today is a team effort



Active Collaborations 2004

- 90 institutions participate
- 425 active users
- 317 scientific authors
- Students and faculty from
  - 65 universities
  - 28 states

US Labs

ANL (Argonne, IL)
LANL (Los Alamos, NM)
LBNL (Berkeley, CA)
LLNL (Livermore, CA)
ORNL (Oak Ridge, TN)
PPPL (Princeton, NJ)
SNL (Sandia, NM)

Industries

Calabasas Creek (CA)
CompX (Del Mar, CA)
CPI (Palo Alto, CA)
Digital Finetec (Ventura, CA)
DRS (Dallas, TX)
DTI (Bedford, MA)
FAR Tech (San Diego, CA)
IOS (Torrance, CA)
Lodestar (Boulder, CO)
SAIC (La Jolla, CA)
Spinner (Germany)
Tech-X (Boulder, CO)
Thermacore (Lancaster, PA)
Tomlab (Willow Creek, CA)
TSI Research (Solana Beach, CA)

US Universities

Auburn (Auburn, Alabama)
Colorado School of Mines (Golden, CO)
Columbia (New York, NY)
Georgia Tech (Atlanta, GA)
Hampton (Hampton, VA)
Lehigh (Bethlehem, PA)
Maryland (College Park, MD)
Mesa College (San Diego, CA)
MIT (Boston, MA)
Palomar (San Marcos, CA)
New York U. (New York, NY)
SDSU (San Diego, CA)
Texas (Austin, TX)
UCB (Berkeley, CA)
UCI (Irvine, CA)
UCLA (Los Angeles, CA)
UCSD (San Diego, CA)
U. New Mexico (Albuquerque, NM)
U. Rochester (NY)
U. Utah (Salt Lake City, UT)
Washington (Seattle, WA)
Wisconsin (Madison, WI)

Russia

Ioffe (St. Petersburg)
Keldysh (Udmurtia, Moscow)
Kurchatov (Moscow)
Moscow State (Moscow)
St. Petersburg State Poly (St. Petersburg)
Triniti (Troitsk)
Inst. of Applied Physics (Nizhny Novgorod)

European Community

Cadarache (St. Paul-lez, Durance, France)
Chalmers U. (Goteberg, Sweden)
CFN-IST (Lisbon, Portugal)
CIEMAT (Madrid, Spain)
Consorzia RFX (Padua, Italy)
Culham (Culham, Oxfordshire, England)
EFDA-NET (Garching, Germany)
Frascati (Frascati, Lazio, Italy)
FOM (Utrecht, The Netherlands)
Helsinki U. (Helsinki, Finland)
IFP-CNdR (Italy)
IPP (Garching, Greifswald, Germany)
ITER (Garching, Germany)
JET-EFDA (Oxfordshire, England)
KFA (Julich, Germany)
Kharkov IPT, (Ukraine)
Lausanne (Lausanne, Switzerland)
IPP (Greifswald, Germany)
RFX (Padova, Italy)
U. Dusseldorf (Germany)
U. Naples (Italy)
U. Padova (Italy)
U. Strathclyde (Glasgow, Scotland)

Japan

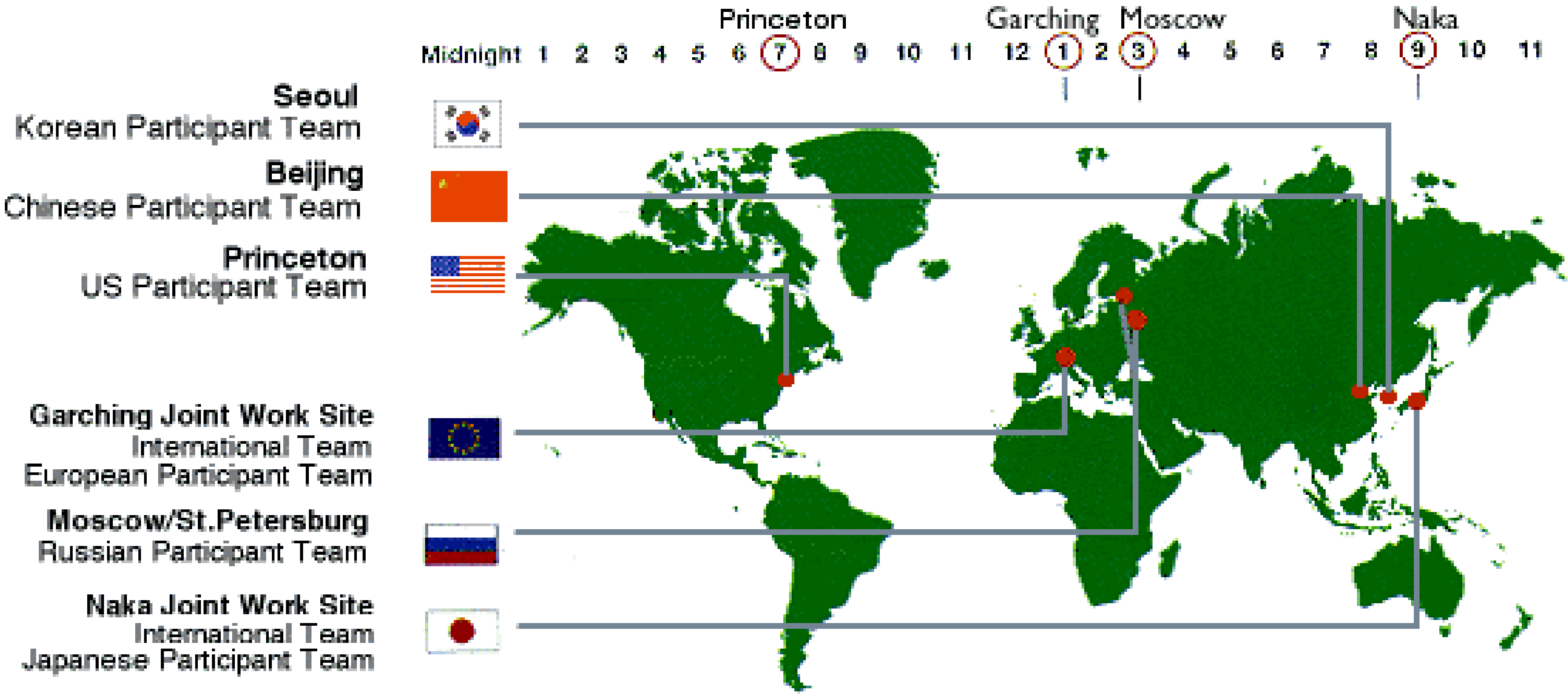
JAERI (Naka, Ibaraki-ken, Japan)
JT-60U
JFT-2M
Tsukuba University (Tsukuba, Japan)
NIFS (Toki, Gifu-ken, Japan)
LHD

Other International

Australia National U. (Canberra, AU)
ASIPP (Hefei, China)
Dong Hau U. (Taiwan)
KBSI (Daegon, S. Korea)
KAERI (Daegon, S. Korea)
Nat. Nucl. Ctr. (Kurchatov City, Kazakhstan)
Pohang U. (S. Korea)
Seoul Nat. U. (S. Korea)
SWIP (Chengdu, China)
U. Alberta (Alberta, Canada)
U. of Kiel (Kiel, Germany)
U. Toronto (Toronto, Canada)

DIII-D has active collaborators on four continents

Fusion research will continue to be a team effort



Seoul
Korean Participant Team

Beijing
Chinese Participant Team

Princeton
US Participant Team

Garching Joint Work Site
International Team
European Participant Team

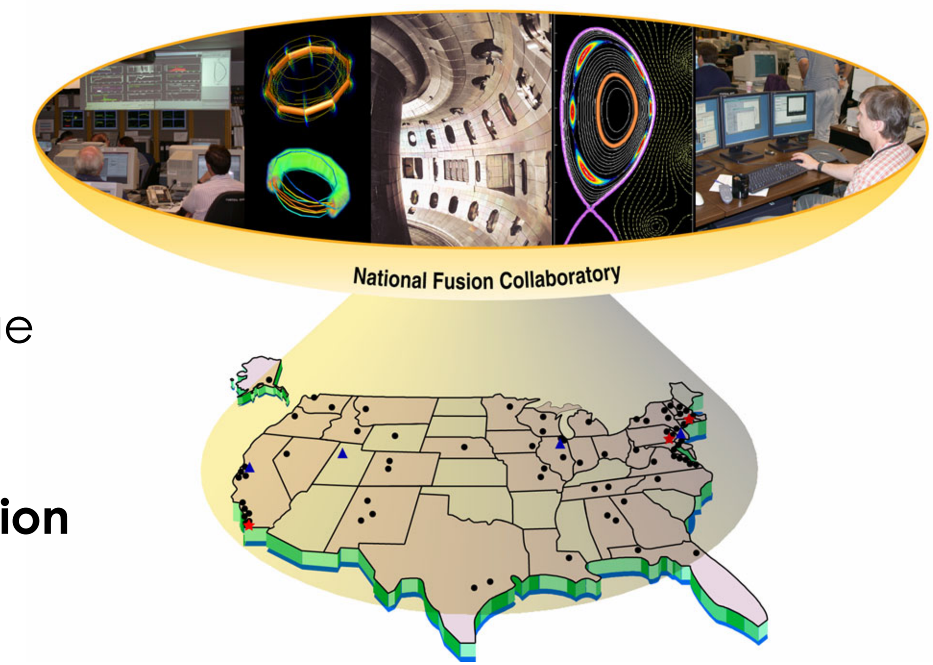
Moscow/St.Petersburg
Russian Participant Team

Naka Joint Work Site
International Team
Japanese Participant Team

The Six ITER Partners

FusionGrid created for better use of resources

- **U. S. Fusion Grid (FusionGrid) aims to make more efficient use of computing resources**
  - Access is stressed rather than portability
  - Not CPU cycle scavenging or "distributed" supercomputing
- **Share resources between sites**
  - Reduce duplication of effort
  - Exploit comparative advantage
- **Develop a common tool set for fusion**
  - Globus Toolkit (GRAM & GSI)
  - Access Grid and VRVS



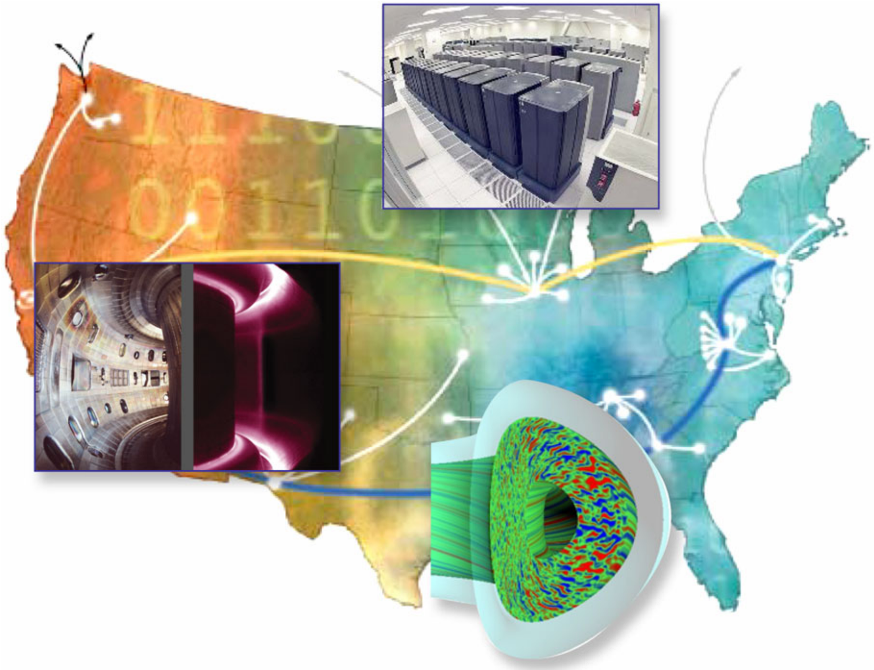
Securing the computational resources of FusionGrid while keeping them usable is the security goal

- **Need to identify FusionGrid users**
  - Tricky as they exist in separate administrative domains

- **Need to allow resource owners to control access to their resources**

- **Starting with first FusionGrid service in 2002, Globus Toolkit used**
  - GSI
  - GRAM
  - grid-mapfiles

- **Was supplemented with Akenti for fine grained authorization**



Problem #1: self-management of credentials was too burdensome to FusionGrid scientists

- **Early use of X.509 certificates demonstrated that requiring each scientist to manage their own credentials was too much of a burden**
  - Browser/platform problems
  - Exporting/converting/installing
  - Had to learn new concept

- **Scientists need to get work done, not figure out how to work with certificates**

- **A solution was needed**
  - Make things simple for the users

Problem #2: authorization relied on grid-mapfiles and lacked a big-picture coherence

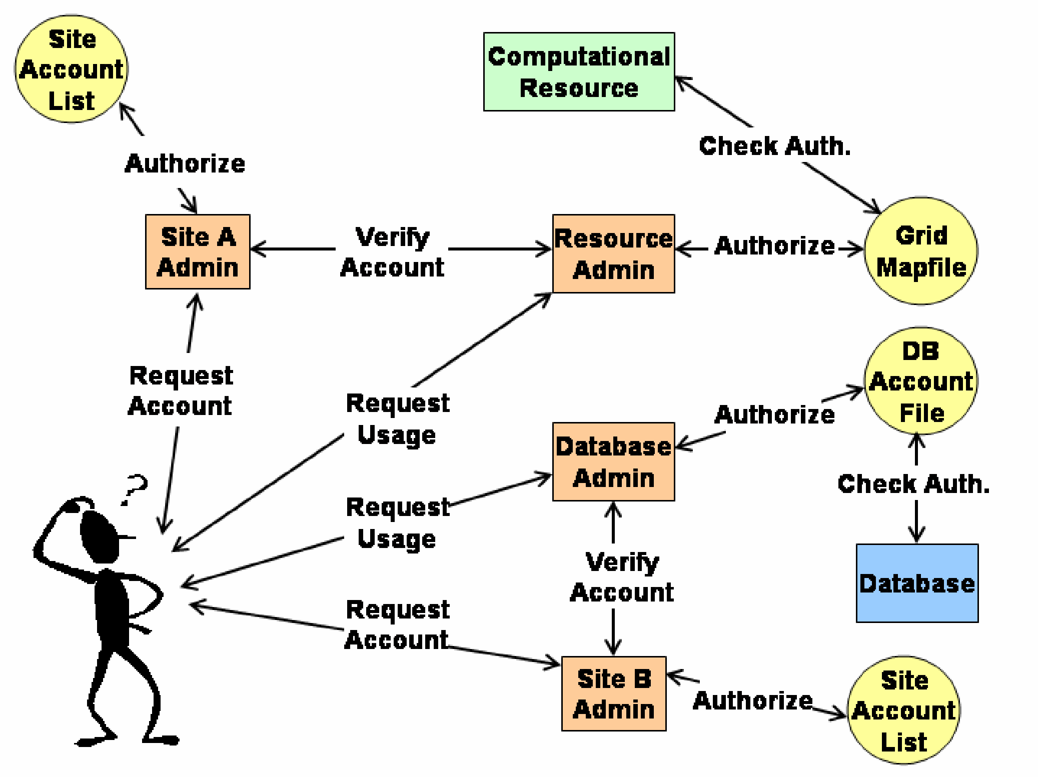
- Site administrators need to control access to their sites

- Resource providers need to control access to their codes/data

- Users just need to get work done

- In this distributed environment it was easy to get lost

- A solution was needed



Security was simplified through a credential manager and a new authorization system

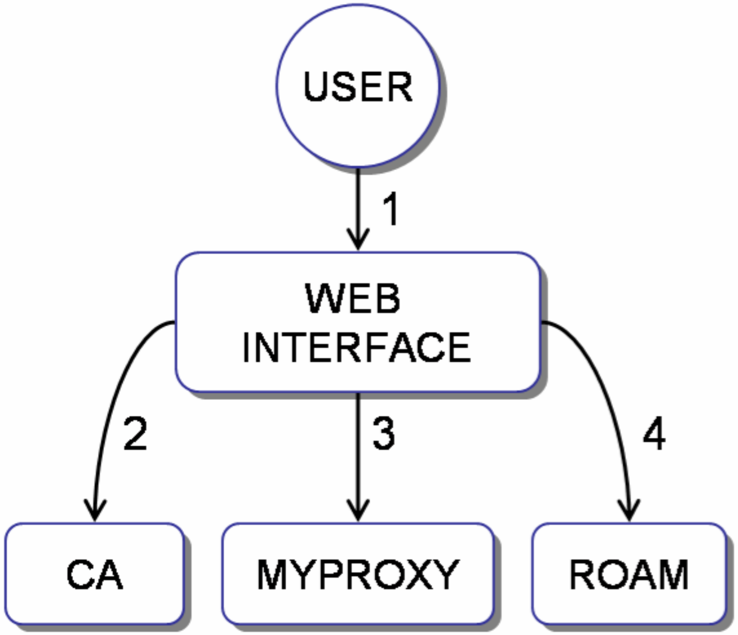
- **Self-management of credentials was too hard for users**
  - Get rid of self-management where possible
    - Use MyProxy to get rid of import/export/installation tasks
  - Make remaining tasks easier
    - Credential manager to request/renew/revoke certs
    - Password hint/change

- **Authorization was too hard for users (and admins)**
  - Created an authorization system (ROAM)
    - Build a coherent model of grid-wide authorization
    - Centralize authorization information
    - Leave room for innovation

Credential manager simplified many tasks

- **MyProxy used to store delegated proxy certificates**
  - Users retrieved delegation when they "sign in" to FusionGrid
  - Username/Password
    - Understood by all

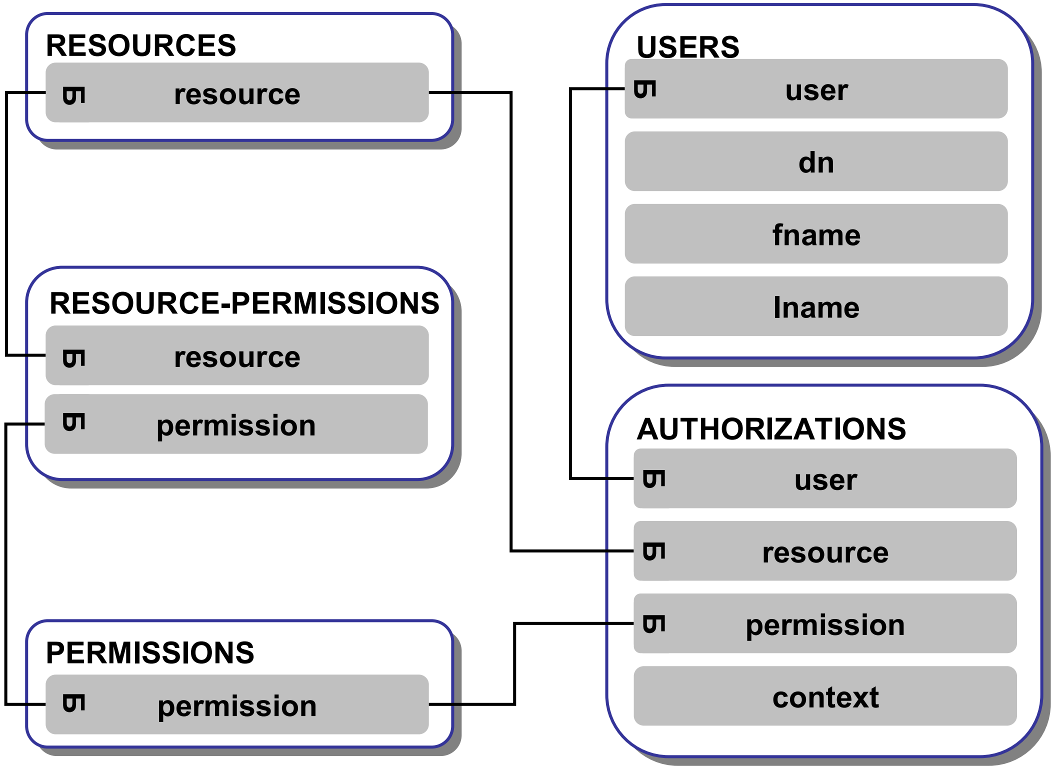
- **Credential manager created simple web interface for many tasks**
  - Request certificate
  - Request password hint
  - Change password



User registration process

A coherent authorization information model laid the foundation for a new authorization system (ROAM)

- Resource Oriented Authorization Manager (ROAM)
- Focus on *resources*
- A resource can be a code, a database, an entire site
- If you have to sign a form to use it, it's probably a resource
- Empower stakeholders to specify types of permissions



RESOURCES
resource

RESOURCE-PERMISSIONS
resource
permission

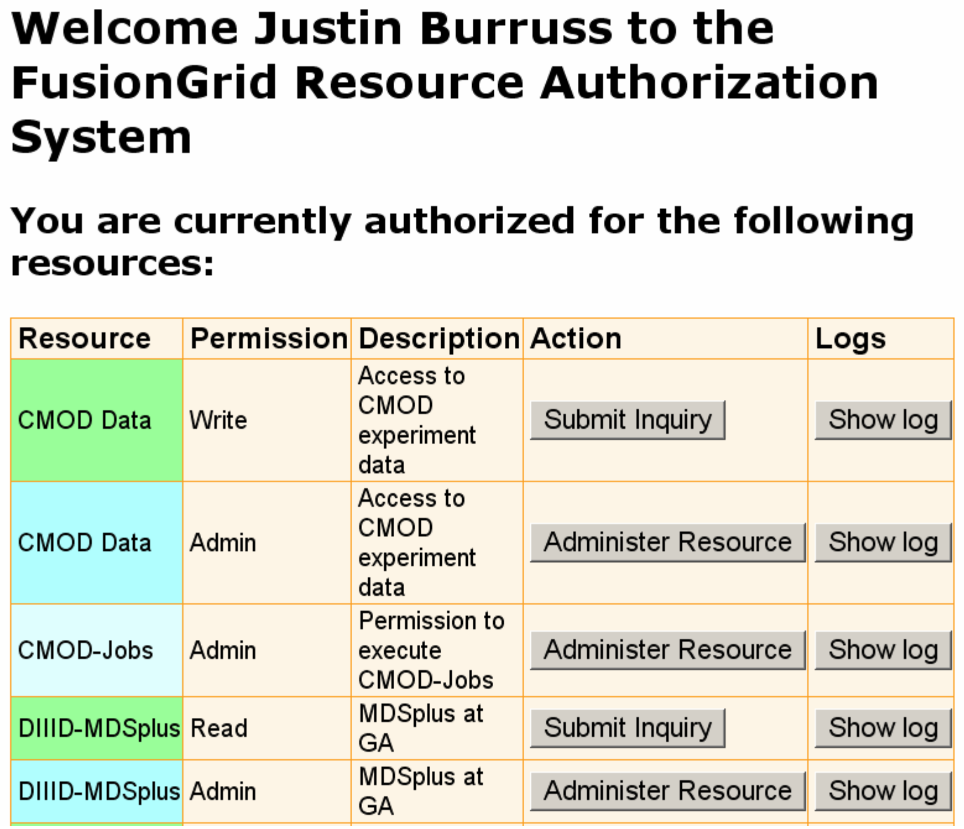
PERMISSIONS
permission

USERS
user
dn
fname
lname

AUTHORIZATIONS
user
resource
permission
context

Users and admins interact with ROAM through a secure web page

- Users request authorization through web page
- Admins grant authorization through same page
- Create new resource or permissions
- View your permissions
- Show log of queries



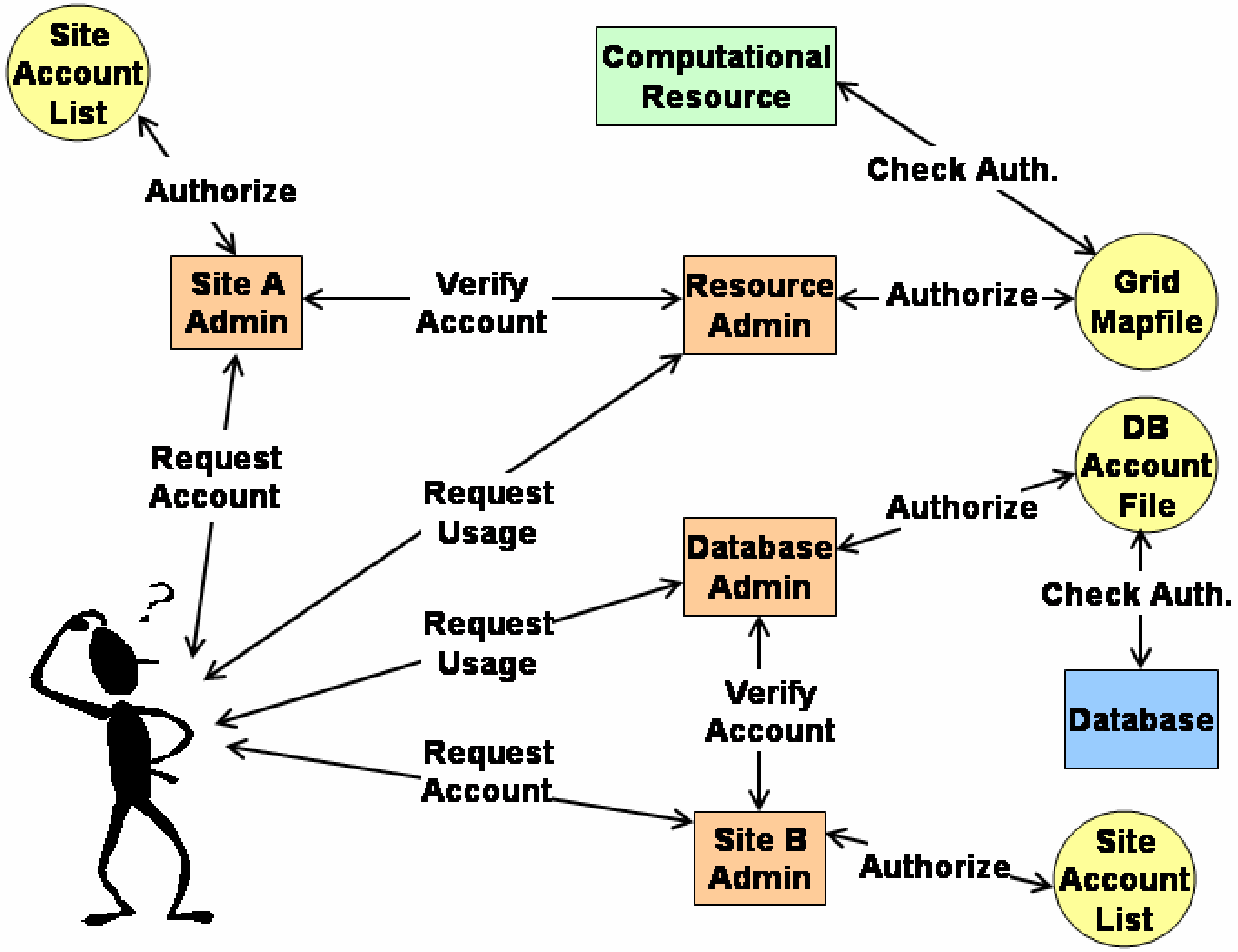
Welcome Justin Burruss to the FusionGrid Resource Authorization System

You are currently authorized for the following resources:

Resource	Permission	Description	Action	Logs
CMOD Data	Write	Access to CMOD experiment data	Submit Inquiry	Show log
CMOD Data	Admin	Access to CMOD experiment data	Administer Resource	Show log
CMOD-Jobs	Admin	Permission to execute CMOD-Jobs	Administer Resource	Show log
DIIID-MDSplus	Read	MDSplus at GA	Submit Inquiry	Show log
DIIID-MDSplus	Admin	MDSplus at GA	Administer Resource	Show log

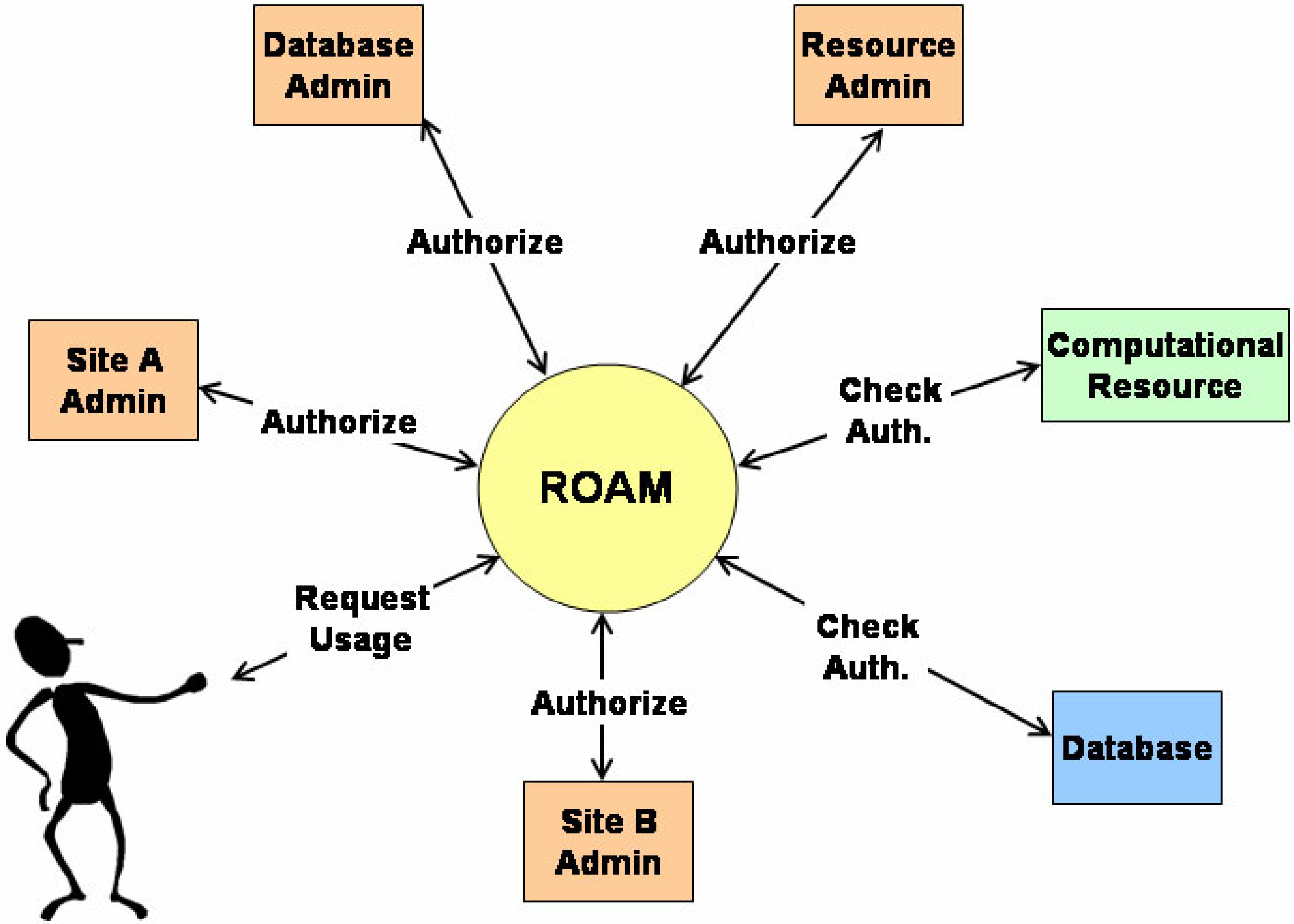
Centralization simplified FusionGrid authorization

- Before



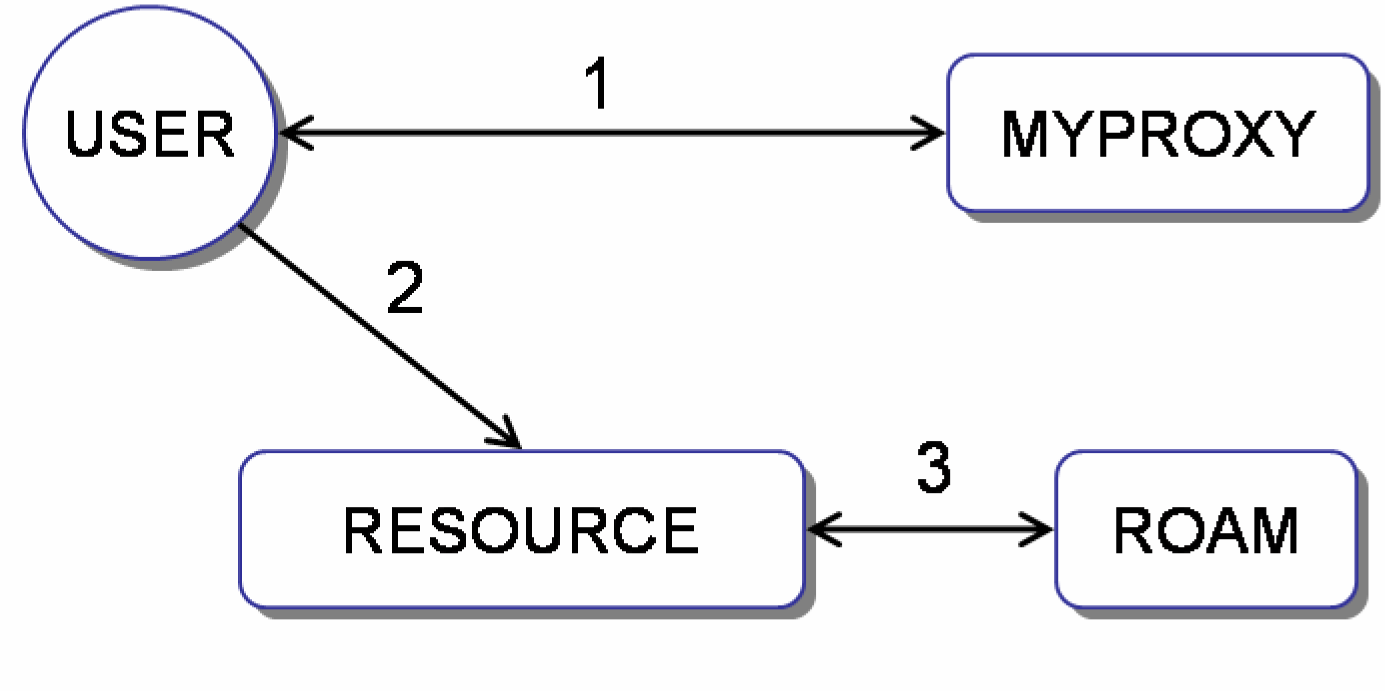
Centralization simplified FusionGrid authorization

- After



ROAM avoids push model of authorization

- User "signs in" as normal, tries to use resource as normal
- Resource queries ROAM for authorization information and makes authorization decision based on that information

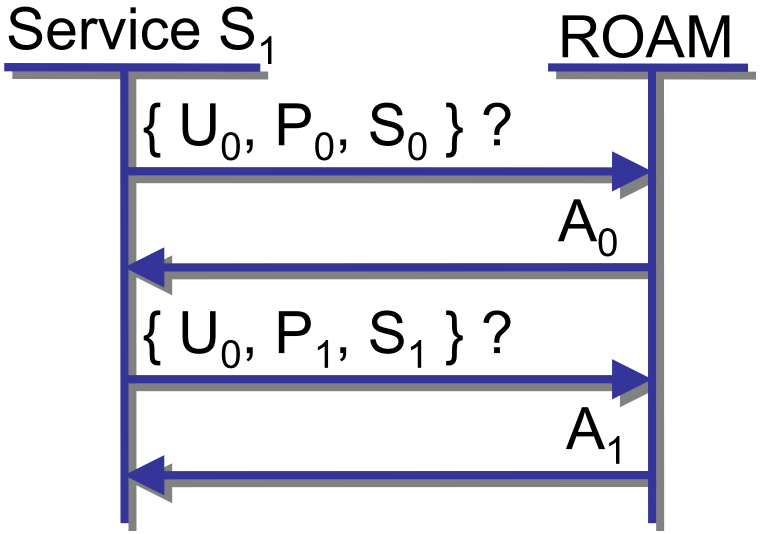


Example: a typical two-rule authorization policy

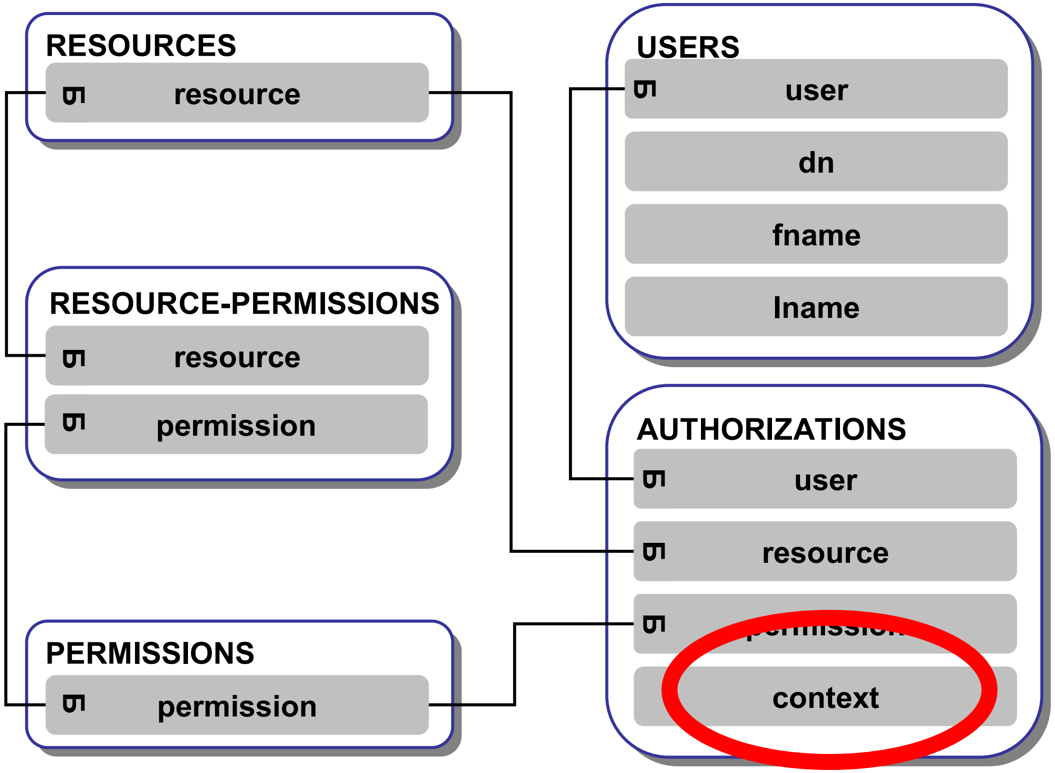
- **Authorization policy for a service S_1 might be**
  1. user must have access permission on site S_0 and
  2. user must have execute permission on code S_1

- **Service sends two queries to ROAM**

- **If answers are both yes, user can use the service**



Context field used for user/group mapping, so no more grid-mapfiles needed



RESOURCES

resource

RESOURCE-PERMISSIONS

resource

permission

PERMISSIONS

permission

USERS

user

dn

fname

lname

AUTHORIZATIONS

user

resource

permission

context

- Context field can be used for anything, but so far is being used for username/group mapping
- GRAM & MDSplus fusion database can call ROAM
- No more grid-mapfiles
- Similarly, no more “mdsip.hosts” files for MDSplus fusion database system

ROAM an easier sell to site admins and developers

- **Site admins reluctant to put access control in hands of "somebody else's" authorization system**

- **But…if you're merely consulting ROAM for authorization information, and letting each resource make decisions based on that information, it's easier to get site admins to adopt**

- **Developers are free to innovate**
  - Could implement complex authorization policies

- **Works well with multiple stakeholders**
  - If you need site access and code permission, both can be modeled and either administrator can stop user

User feedback on new credential management positive

- **Put simply, nobody misses self-management of credentials**
- **Scientists understand the metaphor**
  - username/password needed to “sign on” to grid
  - no new knowledge needed (no training)
  - easier to get work done
- **Other benefits:**
  - Password hint/change has been helpful
  - MyProxy arguably more secure
    - users don’t interact with their files (which are kept on secure server) and instead “sign in”

Next steps

- **Fusion scientists use Mac OS X, Linux, and Windows**
  - Already did a partial port of GSI to Mac OS X ("GSI-lite")
  - Windows will be harder
  - At least a partial GSI port to Windows needed so they can read their data from Windows machines

- **How scalable is ROAM?**
  - Expect model works even if all 2,000+ fusion scientists use it
  - Will it scale to ITER? (next generation fusion device)
  - So far, peak usage very light at 854 queries/hour
  - Will be testing ROAM with a widely-used FusionGrid service to increase usage by order of magnitude

Conclusion: simplification of FusionGrid security made for happier users and administrators

- **The new credential management system is easier for users**
  - No need to learn new metaphor
  - No self-management of credentials
  - Friendly web interface

- **The new authorization system is easier for users, developers, and administrators**
  - Users have one place to go to request permissions
  - Admins have one place to go to set permissions
  - Developers have room to innovate
  - Meets need to allow multiple stakeholders to control access