Open Science Grid

An Introduction to OSG Security

Mine Altunay <maltunay@fnal.gov>
OSG Security Officer
Fermi National Accelerator Laboratory

Who Am I?

- Open Science Grid Security Officer
- Interested in anything related to security
- Alumni of NC State University, Raleigh, PhD in Computer Engineering

What I will talk about

- Basics of security
  - What is authentication
  - What is authorization
  - How what you learned so far is related to security
- How we manage security in OSG?
- What can you do protect yourself?

Open Science Grid

What you learned so far

- Requested a certificate
- Voms-proxy-init
- Submitted jobs
- How it all happened securely? Or maybe was not so secure :)
- What problems did you have so far?
- What was the hardest thing so far?

What does access control mean?

- Security has three pillars
  - Confidentiality, integrity, availability
- How access control fall under this?
  - By managing people's access to resources, security achieves the three pillars
  - Access is granted to people who are authorized to access
  - Needs to know **who** requests access and **whether** they should access or not

Authentication: what are certificates

- Certificate:
  - Bag of bits
  - Similar to a passport. Tells who are you and who gave you this passport (your country vouching for your identity)
- Certificate has
  - Name: /DC=org/DC=doegrids/OU=People/ CN=Alain Roy 424511
  - Expiry date
  - Issuing authority
  - Most importantly your Public Key

Certificate

```
[maltunay@localhost ~]$ openssl x509 -text -in /home/maltunay/.globus/usercert.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 33723 (0x83bb)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: DC=org, DC=DOEGrids, OU=Certificate Authorities, CN=DOEGrids CA 1
        Validity
            Not Before: Jun 22 14:48:28 2009 GMT
            Not After : Jun 22 14:48:28 2010 GMT
        Subject: DC=org, DC=doegrids, OU=People, CN=Mine Altunay 215076
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:9e:93:dc:10:43:07:a2:3c:69:a5:02:c9:0d:7a:
                    a9:8d:a6:4b:f3:77:f3:63:4a:3a:dd:58:a6:5b:02:
                    cb:e6:25:a3:e8:2d:12:53:5f:a6:be:66:ce:43:b4:
                    ae:3c:dd:8d:5a:55:9a:5f:9f:0e:1c:2f:78:b8:51:.....
```

Certificate

-----BEGIN CERTIFICATE-----

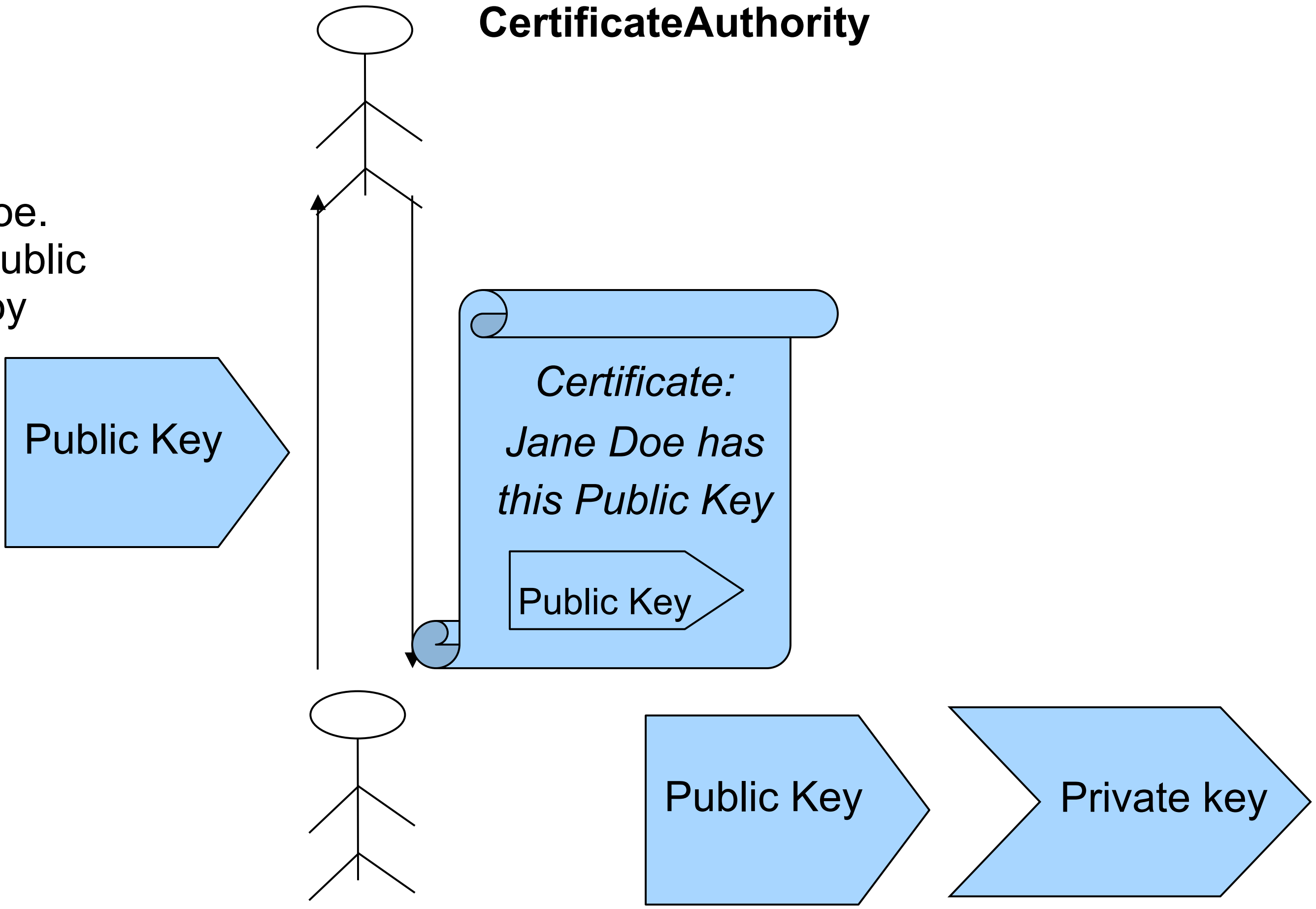
MIIEBDCCAuygAwIBAgIDAIO7MA0GCSqGSIb3DQEBBQUAMGkxEzARBgoJkiaJk/
IsZAEZFgNvcmcxGDAWBgoJkiaJk/
IsZAEZFghET0VHcmlkczEgMB4GA1UECxMXQ2VydGlmaWNhdGUgQXV0aG9yaXRpZXMxFjAU
BgNVBAMTDURPRUdyaWRzIENBIDEwHhcNMDkwNjIyMTQ0ODI4WhcNMTAwNjIyMTQ0ODI4W
jBeMRMwEQYKCZImiZPyLGQBGRYDBeMRMwEQYKCZImiZPyLGQBGRYDb3JnMRgwFgYKCZ
ImiZPyLGQBGRYIZG9lZ3JpZHMxDzANBgNVBAsTBlBlb3BsZTEcMBoGA1UEAxMTTWluZSBBb
HR1bmF5IDIxNTA3NjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJ6T3BBDB6I8
aaUCyQ16qY2mS/N382NKOt1YplsCy+Ylo+gtElNfpr5mzkO0rjzdjVpVml
+fDhwveLhRAJSchgfV8kltofgKN8fKukf0ude6X6eQvLDB0O7j4VUj2a39cg5g/hLBRCo/
78f1IMtXNHLJ8QJkiXQzNSYtNimQU9RFaRiqAwchL
+E7fNjQeZxRj87DQz8xCGYO1eTCV02Kt4KMA4Z6bQ736xR9nQPdb8RxdBi6/
gdP5icIbsuUzHUd5uTlm6dTWG0wAcR27i7mRP3fqZlYXaVshlRou4WTls5s

-----END CERTIFICATE-----

How and why we use certificates?

I am Jane Doe. Here is my public key. Alain Roy knows me.

Give me a certificate

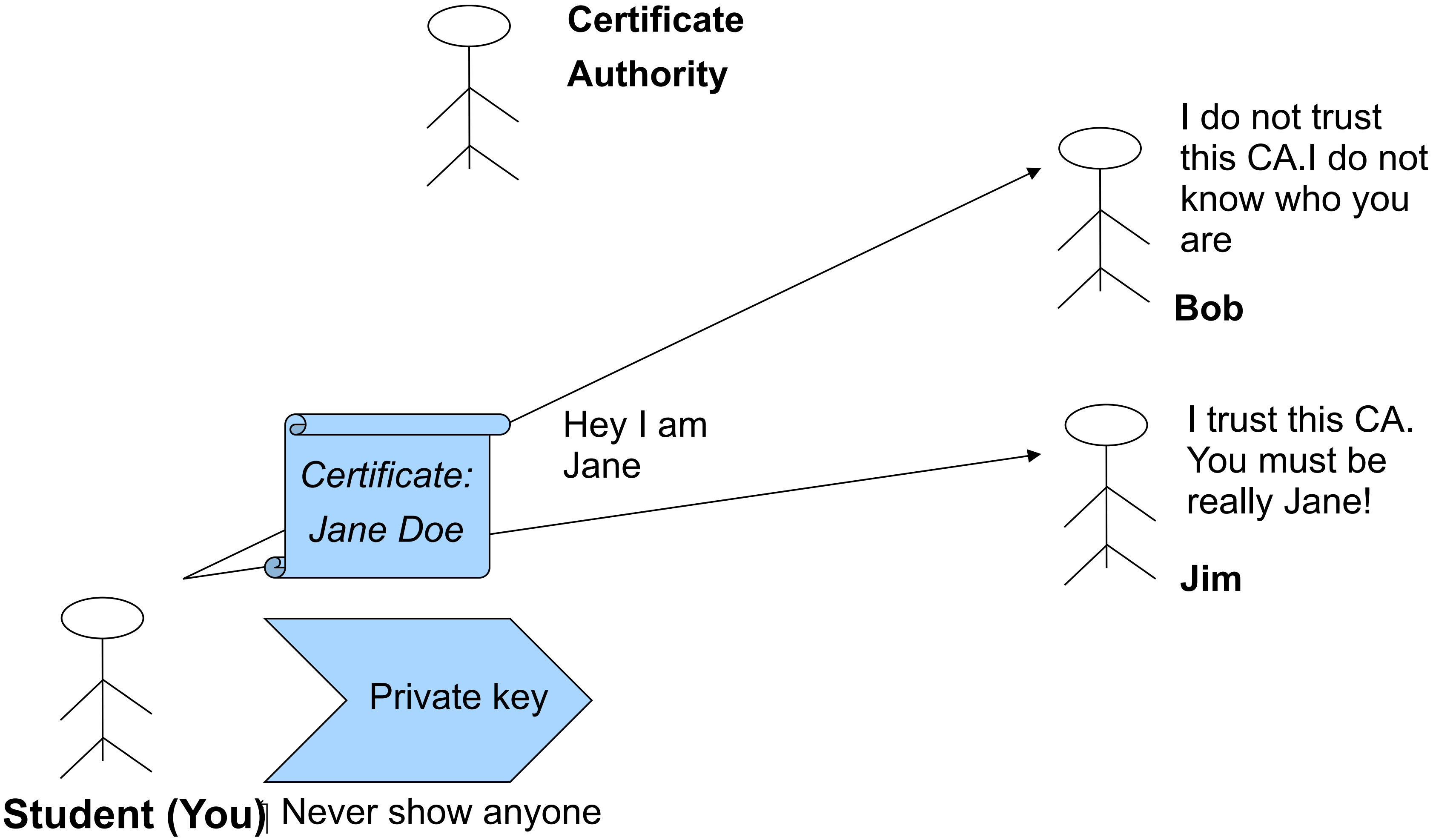


Student (You)

Never show anyone

This is your golden key password

How and why we use certificates?



Certificate Authority

I do not trust this CA.I do not know who you are

Bob

Hey I am Jane

Certificate:

Jane Doe

I trust this CA. You must be really Jane!

Jim

Private key

Student (You)

Never show anyone

This is your golden key password

How certificate works

- Public and secret keys are special
  - They work together. One without the other does not work
- When you need to prove you own a certificate, you
  - send the certificate file (the public key)
  - The other party sends a message encrypted with your public key
  - ONLY you can decrypt the message with your private key
  - send them back the secret message and the other party believe you own the public key

How certificate works

- We use PKI everywhere
- Where else can you think of?
- Can explain what happens when you click on browser exception “are you really sure you trust this web site”

Certificates

- How to care for your certificate
  - Never show anyone your secret key
  - Secret key is encrypted with a password. Do not tell anyone the password
  - Chmod 400 secret-key-file
  - Do not transmit your secret key over unsecure channels, emails, open wireless networks, etc.
  - Certificate and public key is public
  - Use client tools openssl to verify your certificate, check expiry date, check information

What was that voms-proxy-init command for then?

- To generate a proxy
  - A proxy is a short termed certificate you create from your own certificate
  - A proxy on your behalf to act
- Why you need this
  - Ownership of a certificate (private key) is only proven by ownership of secret key.
  - You need to type in your password to unlock the secret key
- Do you want to do this every time you get access to a resource ? NO

Proxy certificate

```
•-----BEGIN CERTIFICATE-----
MIIKPTCCCSWgAwIBAgIDAK8iMA0GCSqGSIb3DQEBBAUAMF4xEzARBgoJkiaJk/Is
ZAEZFgNvcmcxGDAWBgoJkiaJk/IsZAEZFghkb2VncmlkczEPMA0GA1UECxMGUGVv
cGxlMRwwGgYDVQQDExNNaW5lIEFsdHVuYXkgMjE1MDc2MB4XDTEwMDcyMTIwMzgx
M1oXDTEwMDcyMjA4NDMxM1owbjETMBEGCgmSJomT8ixkARkWA29yZzEYMBYGCgmS
-----END CERTIFICATE-----
```

New public key certified **by Jane**

```
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQCuYfQsF1OvpyBJJit8xVyPuMIa3Rg+UEkNQvoaYHVi9Ejg3EC7
hDCtSUDMuc3li/gxMGX0OVQsQpBWJjQinx3pSwDOpY+elqYKES4AV+JUEs5L9xxK
8zILTn9IRinwDwMzB0xj/TPGF2qsrKTgs6DlXyDTyfFyQ4gMyeNJ+pzYYQIDAQAB
AoGAbYUHnUlpPcBw/oACf/JUF8+p2MVTHI+/0ZxnB3ndP7C8tLyfyyVSjQKct/dZ
4Pjvf7Ut0xzOSJ3lmLWVuMjGN1xgkc4IUizbXJMWa0mP7CjfrOv4ynwlIDODtMHa
-----END RSA PRIVATE KEY-----
```

New secret key **(unecrypted)**

```
-----BEGIN CERTIFICATE-----
MIIEljCCAwqgAwIBAgIDAK8iMA0GCSqGSIb3DQEBBQUAMGkxEzARBgoJkiaJk/Is
ZAEZFgNvcmcxGDAWBgoJkiaJk/IsZAEZFghET0VHcmlkczEgMB4GA1UECxMXQ2Vy
dGlmaWNhdGUgQXV0aG9yaXRpZXMxFjAUBgNVBAMTDURPRUdyaWRzIENBIDEwHhcN
Q5eZS5TIfJqCtpKQHkHnIOcxx/qySNS+ATRcd8LqVQDcbrR5Yf3swVycOff6QMRY
YH6RpueE0tb1zeJ+1OcJOhBWqnSyRLnpVJwkBmFktsX2kBIhO01QGA7yAT0YEyHO
H0RS/URc
-----END CERTIFICATE-----
```

Jane's own certificate

Proxy certificates

- Basically it is delegation
  - Give the proxy to a process that accesses resources on your behalf for 12 hours while you go drink coffee
  - Similar to a power of attorney
- Is there any protection on proxy?
  - NO!
  - The process runs while you drink coffee has full access to the proxy. If the process runs on a remote machine remote machine has your proxy
  - If the remote machine is not secure, anyone else has your proxy and claims to work for you

Proxy Certificates

- What do we do?
- Make the proxy short-termed
  - Only for the duration of the job
  - voms-proxy-init   -valid <h:m>
- Make the proxy limited
  - voms-proxy-init -limited
  - Limited proxy cannot spawn a new job on your behalf, but can only do data transfer
  - Eliminates the risk if someone steals your proxy

So Far

- Questions,
- More details or too complex?
- Should we move on?

Open Science Grid

What is Authorization?

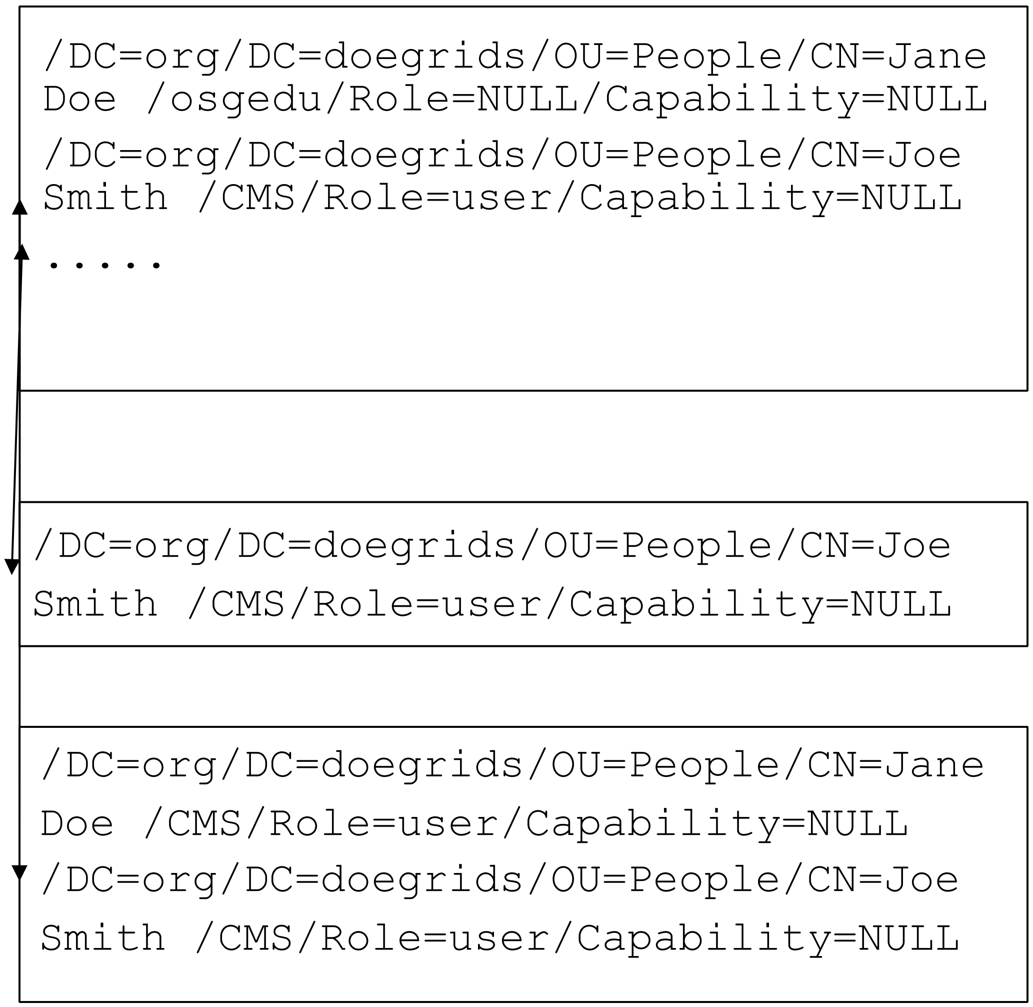
- Authorization is the act of allowing **someone** to perform **actions** one a **resource**
- How does it differ from authentication?
  - Authentication does not care which actions you can perform on what resources
  - Authentication only cares who you are, your identity
  - Authorization takes your identity from authN and makes a decision whether you should access a resource or not
- Why do you care?

Open Science Grid

What is that voms thing in voms-proxy-init: Authorization

- A VO is a group of people working together
- OSG sites give access to VOs, not individuals
- You should be a member of a VO to access a site
- VOMS is the VO management service that keeps track of VO members
- Sites download the list from each VO

Authorization and VOMS



/DC=org/DC=doegrids/OU=People/CN=Jane Doe /osgedu/Role=NULL/Capability=NULL

/DC=org/DC=doegrids/OU=People/CN=Joe Smith /CMS/Role=user/Capability=NULL

.....

VOMS

/DC=org/DC=doegrids/OU=People/CN=Joe Smith /CMS/Role=user/Capability=NULL

Authorized user list for **CE1** supporting CMS only

/DC=org/DC=doegrids/OU=People/CN=Jane Doe /CMS/Role=user/Capability=NULL

/DC=org/DC=doegrids/OU=People/CN=Joe Smith /CMS/Role=user/Capability=NULL

Authorized user list for CE2 supporting CMS and Edu VO

Authorization and VOMS

- When you do voms-proxy-init
  - You generate a proxy certificate
  - Send it to VOMS server
  - VOMS server checks if you are really Jane Doe (you have the certificate)
  - VOMS server puts another stamp in your proxy “Jane Doe really belongs to Education VO of OSG”
- But then your proxy has been changed?
- And how does a site know this is really the Education VOMS server, not the Mike the attacker's VOMS server

Authorization and VOMS

- Your proxy is changed, but only in the extensions field
  - Its integrity is kept
- Each VOMS has their own certificates
- The sites can check whether the stamp in Jane's proxy matches the Edu VOMS server's certificate
- This is a digital signature, just a bunch of digits

```
[maltunay@localhost osg-ce-latest]$ openssl x509 -text -in /tmp/x509up_u500
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 44834 (0xaf22)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: DC=org, DC=doegrids, OU=People, CN=Mine Altunay 215076
        Validity
            Not Before: Jul 21 20:38:13 2010 GMT
            Not After : Jul 22 08:43:13 2010 GMT
            Subject: DC=org, DC=doegrids, OU=People, CN=Mine Altunay 215076, CN=proxy
            Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
            Modulus (1024 bit):
                    00:ae:61:f4:2c:17:53:af:a7:20:49:26:2b:7c:c5:
                    7f:48:46:29:f0:0f:03:33:07:4c:63:fd:33:c6:17:
                    6a:ac:ac:a4:e0:b3:a0:e5:5f:20:d3:c9:f1:72:43:
                    88:0c:c9:e3:49:fa:9c:d8:61
                Exponent: 65537 (0x10001)
```

```
X509v3 extensions:
          1.3.6.1.4.1.8005.100.100.5: .
..U....People1.0...U....Mine Altunay 215076....".e0c.a0_1.0..
..&...,d....org1.0............:.0"..20100721204333Z..20100722084333Z0..0...voms.fnal.gov0
+.....Edd.1u0s...fermilab://voms.fnal.gov:150010O.#/fermilab/Role=NULL/Capability=NULL.(/fermilab/test/Role=NULL/
Capability=NULL0..z0..
100910192438Z0_1.0..1 0...U....Certificate Authorities1.0...U...
..&...,d....org1.0..
..........0..oegrids1.0...U....Services1.0...U....http/voms.fnal.gov0.."0
T.j........H.i..T.I....B/.............6.e.jZ.[.TymG......BK..........,..Z.2!.@2.......1!...]..n...Q..........*.H..L....0.0
          X509v3 Key Usage: critical
             Digital Signature, Key Encipherment, Data Encipherment
          1.3.6.1.4.1.8005.100.100.6:
             03
-----BEGIN CERTIFICATE-----
MIIKPTCCCSWgAwIBAgIDAK8iMA0GCSqGSIb3DQEBBAUAMF4xEzARBgoJkiaJk/Is
ZAEZFgNvcmcxGDAWBgoJkiaJk/IsZAEZFghkb2VncmlkczEPMA0
-----END CERTIFICATE-----
```

How to get information on your proxies

- voms-proxy-info is your friend

```
subject   : /DC=org/DC=doegrids/OU=People/CN=Mine Altunay 215076/
    CN=proxy
issuer    : /DC=org/DC=doegrids/OU=People/CN=Mine Altunay 215076
identity  : /DC=org/DC=doegrids/OU=People/CN=Mine Altunay 215076
type      : proxy
strength  : 1024 bits
path      : /tmp/x509up_u500
timeleft  : 7:09:06
```

- By default
  - Your certificate is under /home/.globus
  - usercert.pem and userkey.pem
  - Your proxy is under /tmp/xup_500

- Is this limited proxy or not?
  - Try another command
  - grid-proxy-info

```
subject  : /DC=org/DC=doegrids/OU=People/CN=Mine Altunay 215076/CN=proxy
issuer   : /DC=org/DC=doegrids/OU=People/CN=Mine Altunay 215076
identity : /DC=org/DC=doegrids/OU=People/CN=Mine Altunay 215076
type     : full legacy globus proxy
strength : 1024 bits
path     : /tmp/x509up_u500
timeleft : 7:05:45

subject  : /DC=org/DC=doegrids/OU=People/CN=Mine Altunay 215076/CN=795946817
issuer   : /DC=org/DC=doegrids/OU=People/CN=Mine Altunay 215076
identity : /DC=org/DC=doegrids/OU=People/CN=Mine Altunay 215076
type     : Proxy draft (pre-RFC) compliant limited proxy
strength : 512 bits
path     : /tmp/x509up_u500
timeleft : 11:59:50
```

How to know something fishy going on

- OSG keeps track of per user job records
  - You can get your own job record
  - If a job has run under your name when you are on vacation, that is strange
- Do not use your private key on insecure machines (someone else's laptop, internet kiosk, etc)
- Go to http://gratia-osg.fnal.gov:8880/gratia-reporting/
  - Run a mysql query
  - select * from VOProbeSummary? where CommonName? like "%wenjing wu%"
  - Will list all jobs running under your proxy

Open Science Grid

What to do if something goes wrong?

- Let's say your computer is infected
- Let us know:
  - security@opensciencegrid.org
  - Call 1 317-278-9699
- We will find if someone impersonate you and revoke your old certificate and give you a new one

Open Science Grid

What else could go wrong?

- Jobs fail due to security issues
- The error codes are not very verbose
- This is a good guide
- http://vdt.cs.wisc.edu/tmp/jobs_not_running_admin.html
- Reverse DNS look up error
  - The site has a DNS alias, but its certificate does not match the alias
  - globus-job-run localhost::/DC=org/DC=doegrids/OU=Services/CN=null-00188bda7c28.dhcp.fnal.gov /bin/date

- globus-url-copy -a -nodcau -ss

/DC=org/DC=doegrids/OU=Services/CN=null-00188bda7c28.dhcp.fnal.gov

gsiftp://localhost/home/maltunay/.globus/test

file:/home/maltunay/.globus/test2

- Nodcau means no data channel authentication for performance reasons
- -ss is service subject to overcome reverse dns lookup
- Are you sure you show up in VOMS server
  - When you get a new certificate, you should tell your VOMS admin to add this to the VO
  - If not, site will not allow access

Open Science Grid

What if you need certificates in the web?

- You may need to import/export your certificates into your browser and email client
- Needed for secure communication, and access control to services needing PKI