
# Security in OSG

## Tuesday afternoon

Igor Sfiligoi <isfiligoi@ucsd.edu>
University of California San Diego

# Logistical reminder

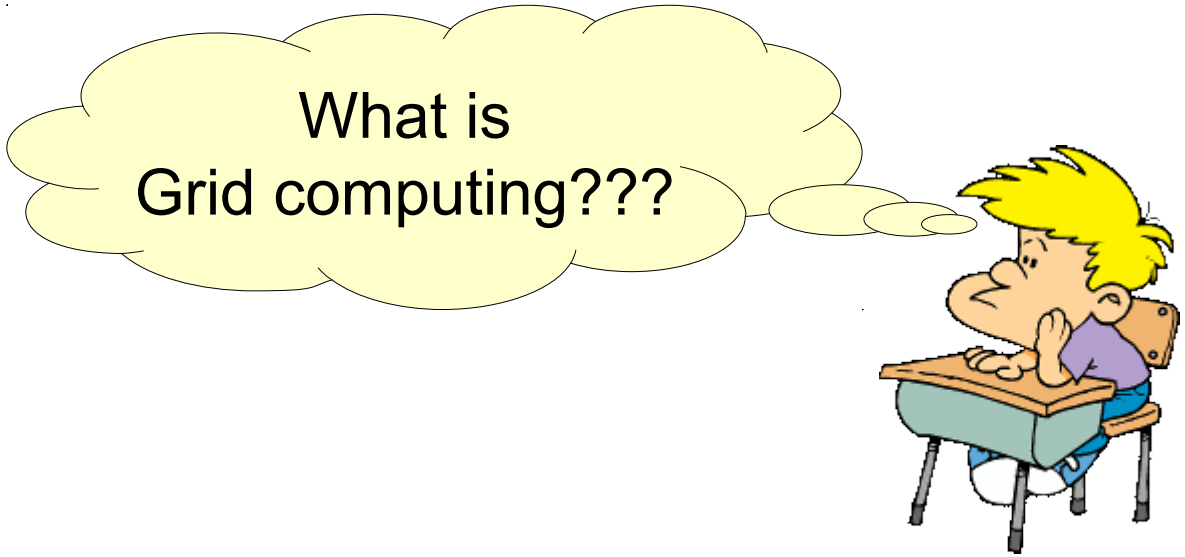
- It is OK to ask questions
  - During the lecture
  - During the demos
  - During the exercises
  - During the breaks
- If I don't know the answer,
  I will find someone who likely does

# The Open Science Grid

- The Open Science Grid is an organization promoting Distributed HTC
- Its main focus is on enabling Grid computing in the USA

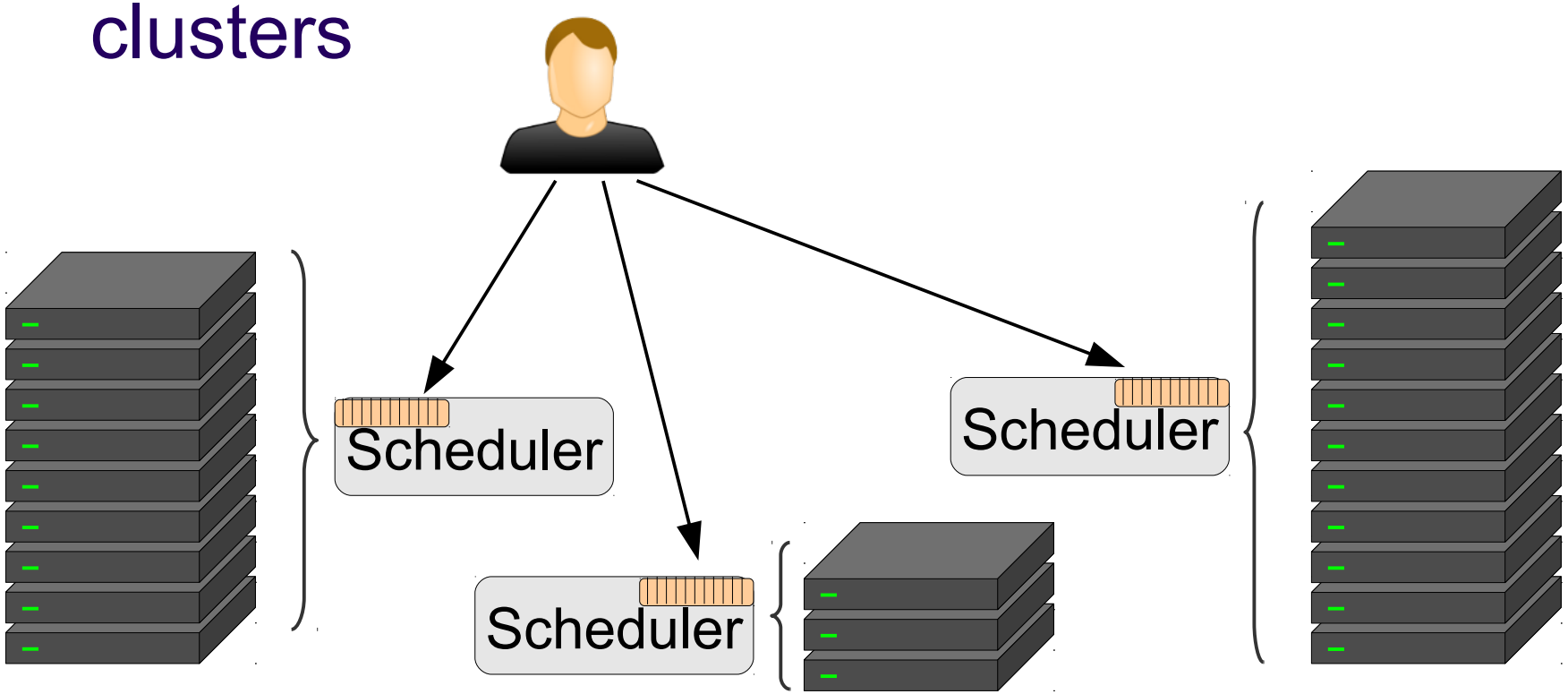
# The Open Science Grid

- The Open Science Grid is an organization promoting Distributed HTC
- Its main focus is on enabling Grid computing in the USA



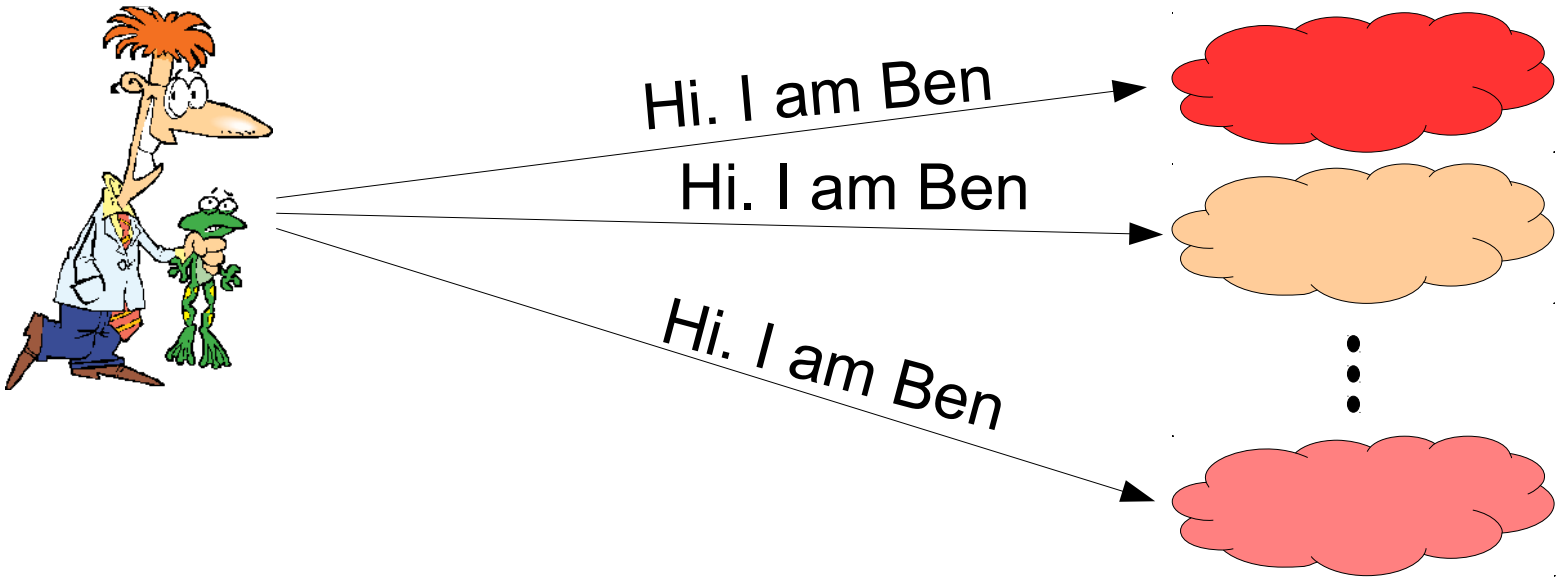
# Grid and DHTC

- Grid, as a form of DHTC, is about enabling computing on remote HTC clusters



# Single sign-on

- Main contribution of Grid to DHTC is availability of single sing-on
  - Users have a single identity on each and every Grid site



# OSG Auth not password based

- OSG not using password authentication
  - For several reasons
- For starters, it is effectively a **shared secret** between **the user and the service provider**
  - And secrets stay secret only if few entities know it
  - Imagine sharing passwords between 100s of site operators

# Adding an intermediary

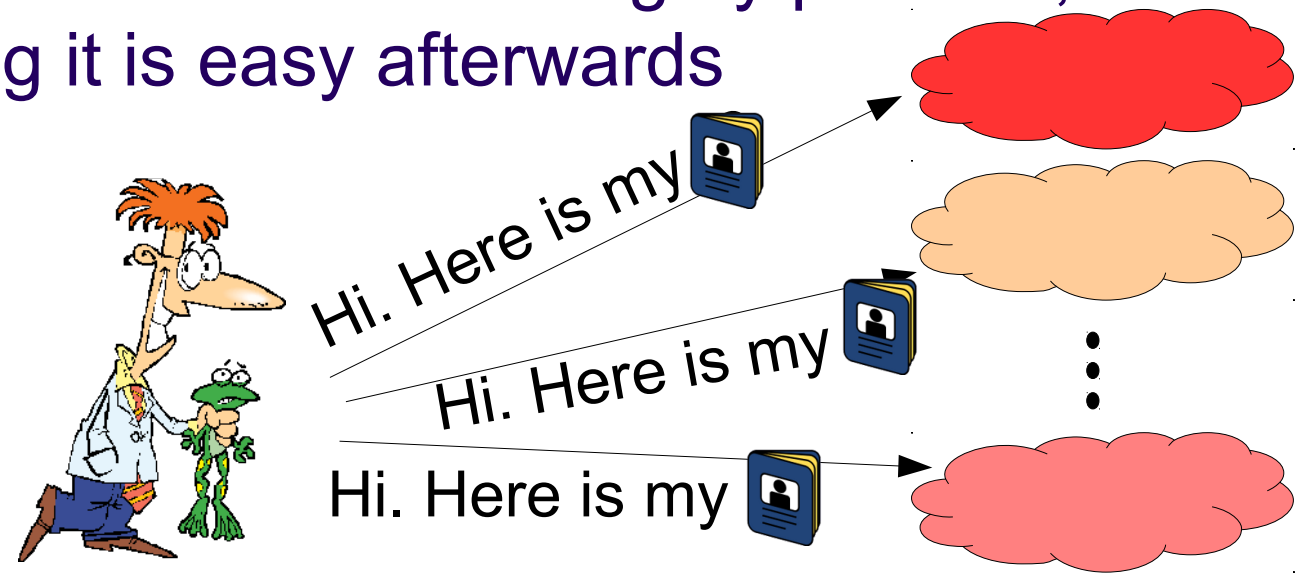
- An alternative approach is to introduce a highly trusted intermediary
- Have been used in real life for ages
  - e.g. States as issuers of IDs/Passports

# Adding an intermediary

- An alternative approach is to introduce a highly trusted intermediary
- Have been used in real life for ages
  - e.g. States as issuers of IDs/Passports
  - Getting the ID can be a lengthy process

# Adding an intermediary

- An alternative approach is to introduce a highly trusted intermediary
- Have been used in real life for ages
  - e.g. States as issuers of IDs/Passports
  - Getting the ID can be a lengthy process, but using it is easy afterwards



# Adding an intermediary

- An alternative approach is to introduce a highly trusted intermediary
- Have been [illegible] for ages
  - e.g. [illegible]
  - [illegible]

Chain of trust.

You are trusted because the site trusts the issuer, and the issuer trusted you.

# Technical implementation

- OSG uses the x.509 PKI
  - A user gets **a certificate file**
  - Issued by a Certification Authority (CA)
- Like a real passport, a certificate
  - Contains your name
  - Has an **expiration date**
    - Typically issued for one year

# Authentication vs. Authorization

- Just because you can authenticate yourself, it does not mean you are authorized, too
  - e.g. your passport tells who you are, but does not allow you to drive a car
- x.509 PKI only covers **authentication**
  - Tells the site who you are
- We need a different mechanism for authorization

# Adding a user type

- Keeping a whitelist not an option
  - Just too many users
- Want to authorize on the type of user
  - There should be just a few of them

# Adding a user type

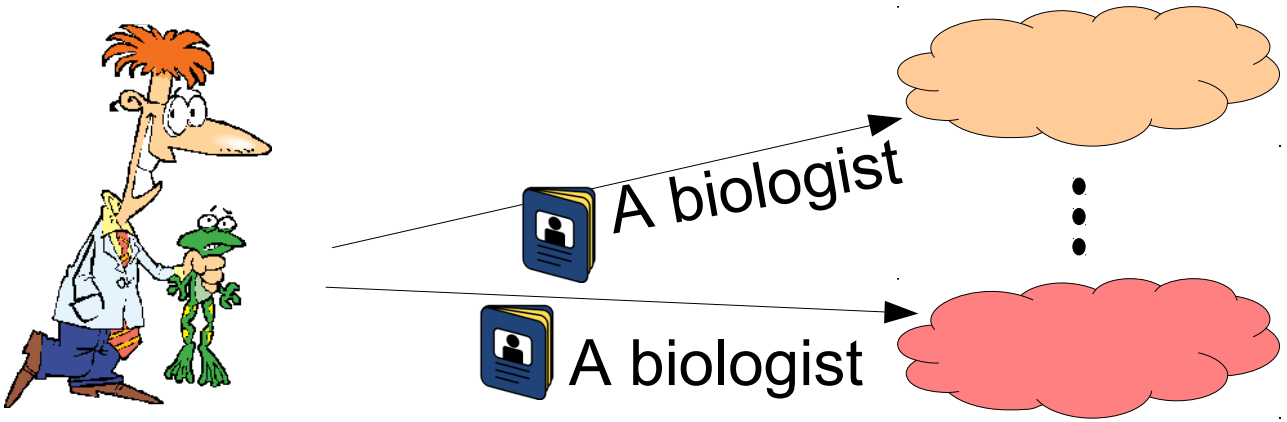
- Keeping a whitelist not an option
- Want to authorize on the type of user
  - There should be just a few of them
- Let's imitate real life again
  - Think about **passport vs driver's license**
  - Both tell a cop who you are
    (and to 1st approx. are issued by the same entity)
  - But the driver's license tells him
    you are **allowed to use a car, too**
    - **“Class:C”**

# Virtual Organizations

- In OSG, we reason in terms of Virtual Organizations (VOs)
- Each VO represents a user type, e.g.
  - Physicist in the CMS LHC experiment
  - User of the UW Madison campus
- All users of a VO are to be considered equivalent
  (there may be exceptions, but we will not delve into this)

# VOMS Attributes

- Technically, each VO runs a VOMS
  - The VO keep the whitelist of its own users
- A VOMS will **extend a user certificate**
  - **Adding an attribute certifying** that the user belongs to this VO
- This information is then used by the sites

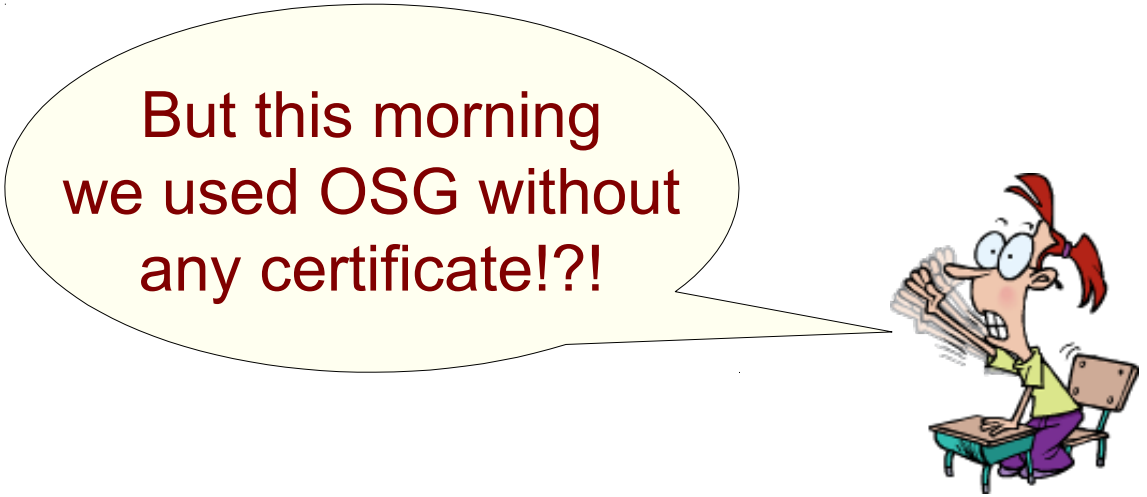


# OSG is x.509 based

- Bottom line,
  the OSG security infrastructure
  is based on
  VOMS-extended x.509 certificates

# OSG is x.509 based

- Bottom line,
  the OSG security infrastructure
  is based on
  VOMS-extended x.509 certificates



# OSG and overlays

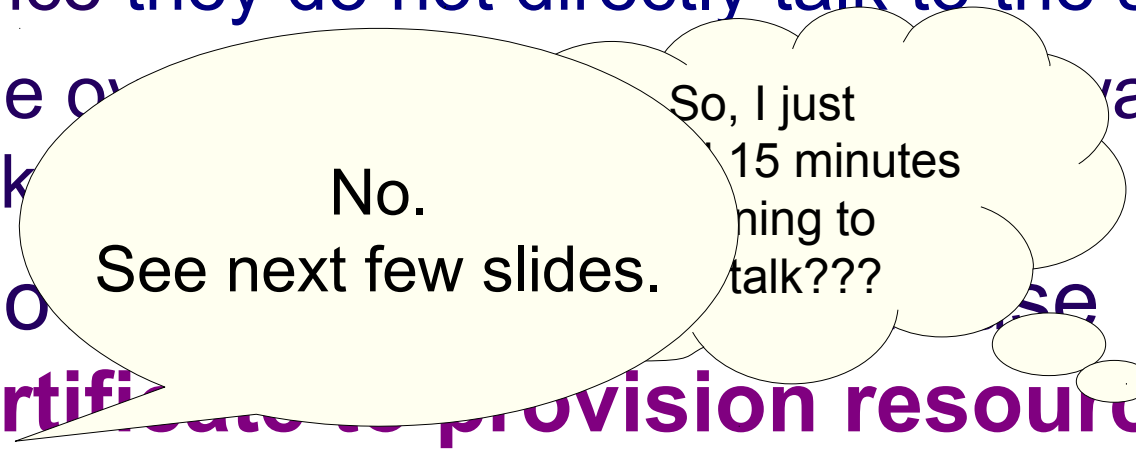
- When using DHTC overlays, users don't need a certificate
  - Since they do not directly talk to the sites
  - The overlay system can use other ways to keep track of its users
- The overlay administrator will use **a certificate to provision resources** that joined the overlay system
  - But this is not tied to any final user

# OSG and overlays

- When using DHTC overlays, users don't need a certificate
  - Since they do not directly talk to the sites
  - The overlay syste… …ays to keep track of …
- The overlay admin… …se **a certificate to provision resources** that joined the overlay system
  - But this is not tied to any final user

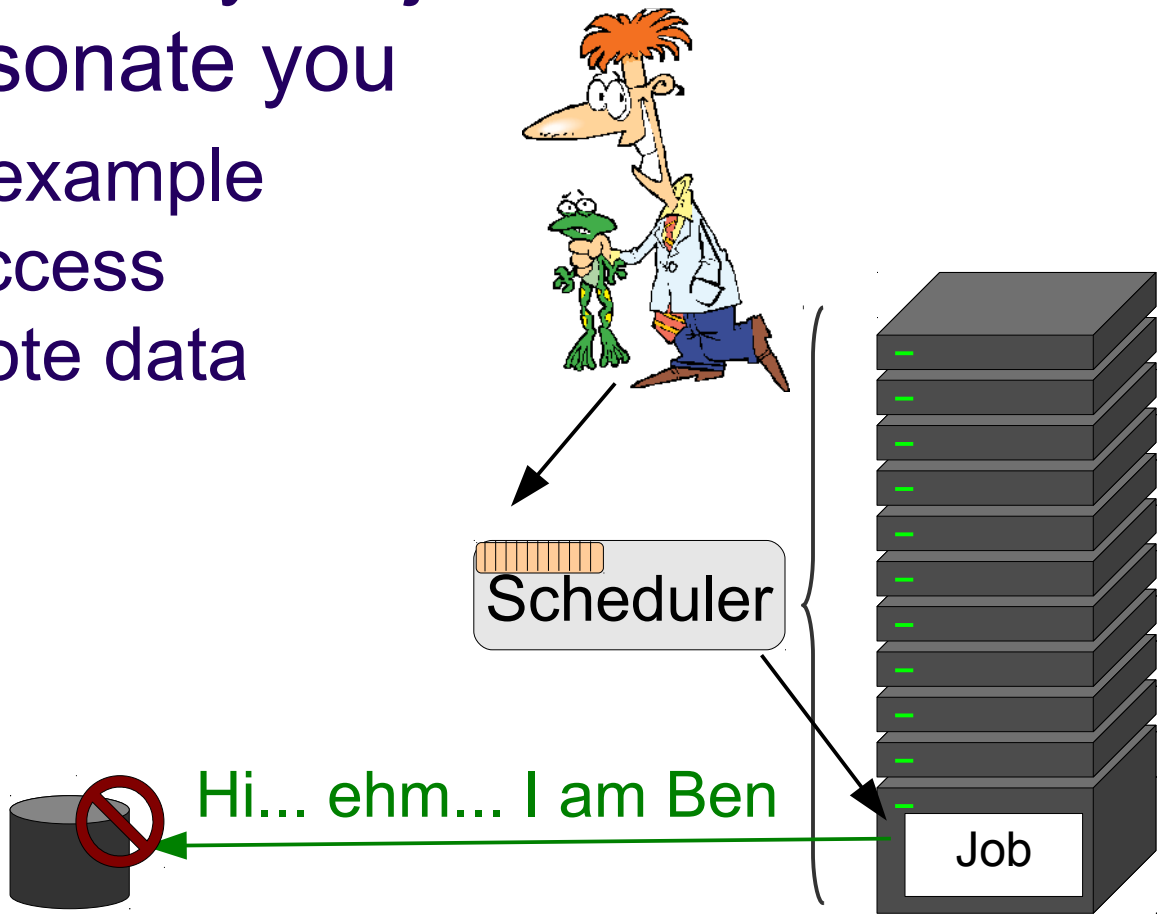
# OSG and overlays

- When using DHTC overlays, users don't need a certificate
  - Since they do not directly talk to the sites
  - The o… …ays to k…
- The o… …se a certificate to provision resources
  - …joined the overlay system
  - But this is not tied to any final user



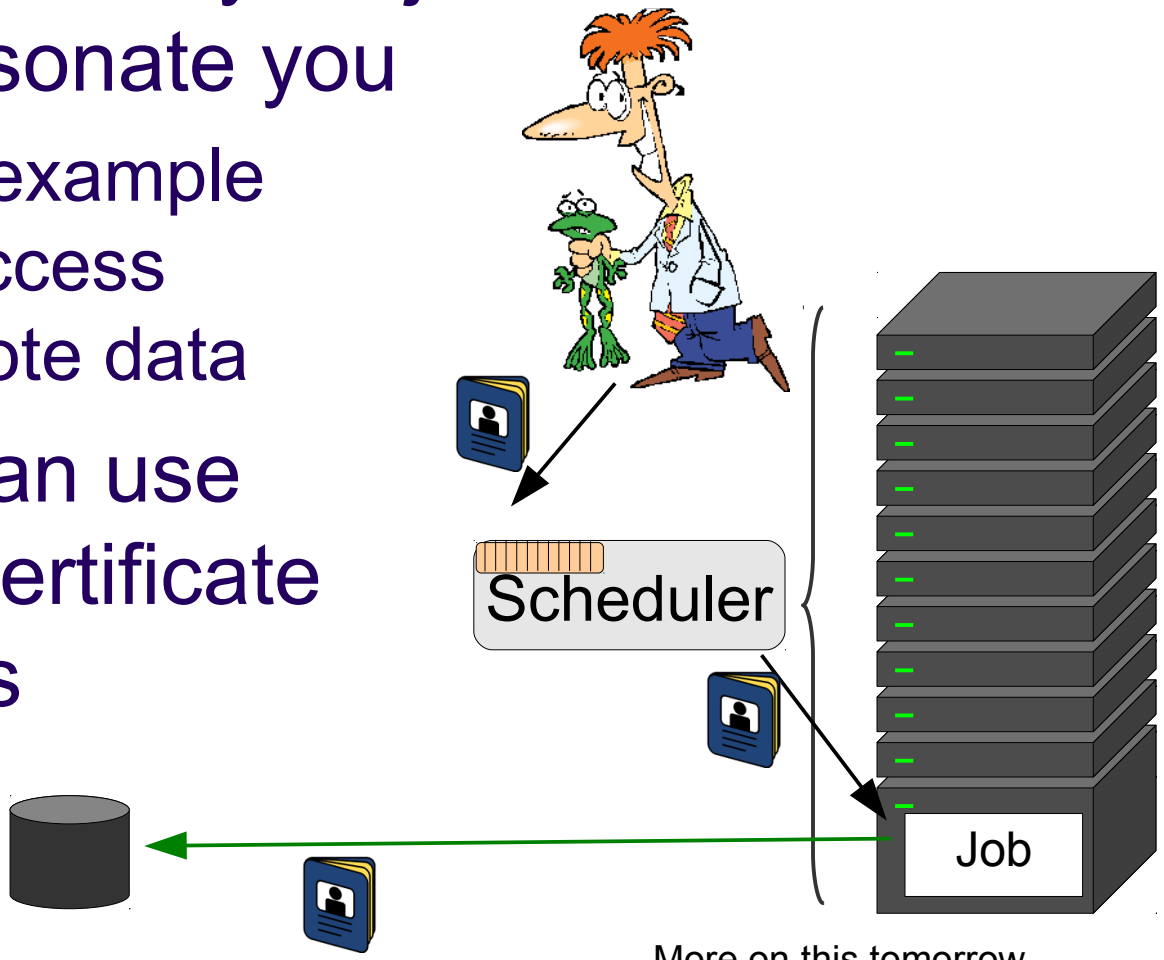

# Impersonation

- Sometimes your jobs need to impersonate you
  - For example to access remote data



# Impersonation

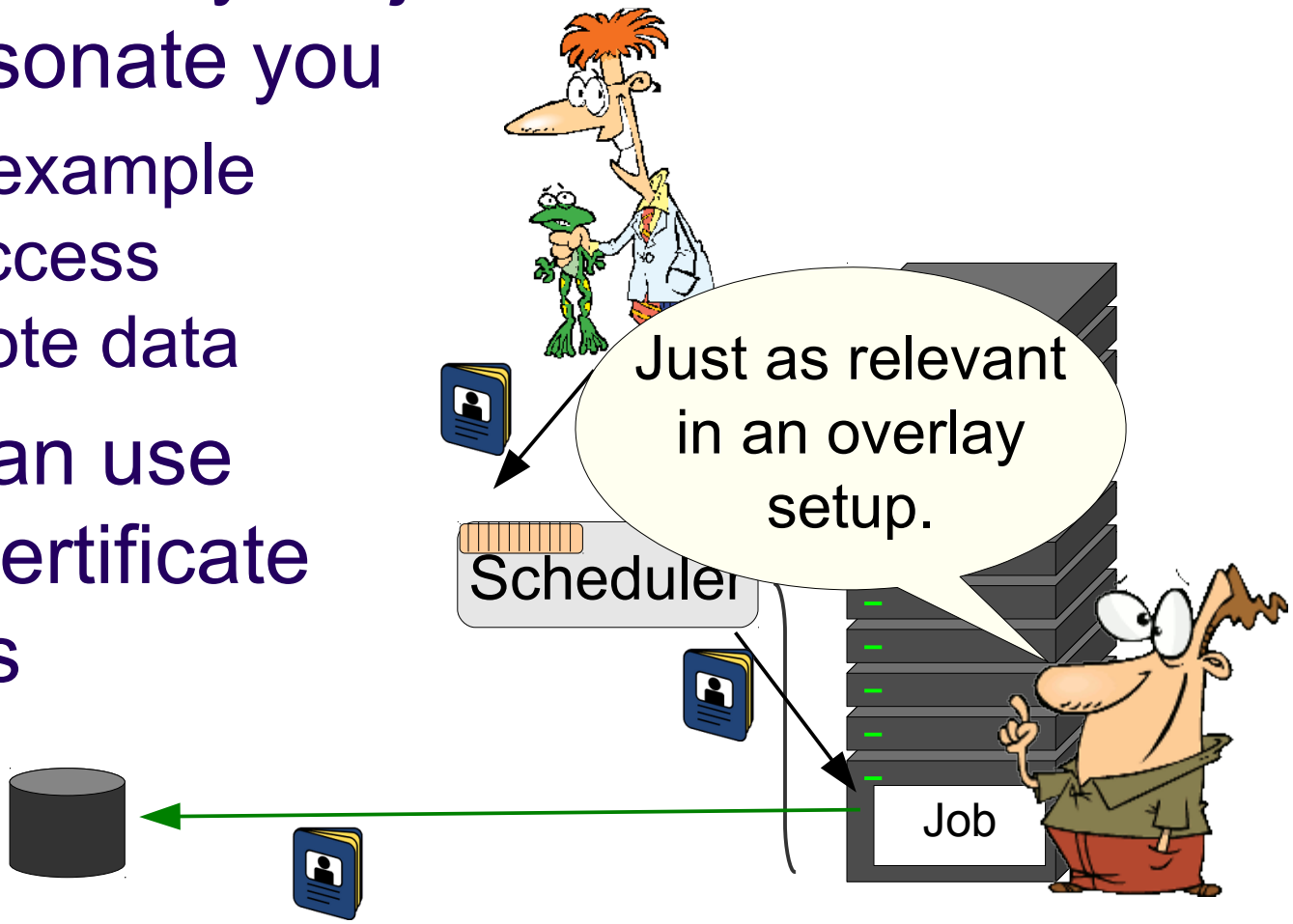
- Sometimes your jobs need to impersonate you
  - For example to access remote data
- You can use your certificate for this




More on this tomorrow.

# Impersonation

- Sometimes your jobs need to impersonate you
  - For example to access remote data
- You can use your certificate for this



# More security considerations

- There is much more than authentication and authorization to security
  - But we don't have the time to cover everything
- Just briefly
  - Sharing of resources
  - Privacy
  - Acceptable conduct

# Sharing of resources

- Modern CPUs are many-core, so
  - Very likely your job will be sharing the node with other jobs
- No guarantee that there will be any protection between you and other jobs from users of the same VO
  - But should be protected from other VOs
- Limited OS level protections
  - Act accordingly
  - e.g. no file should be world writable

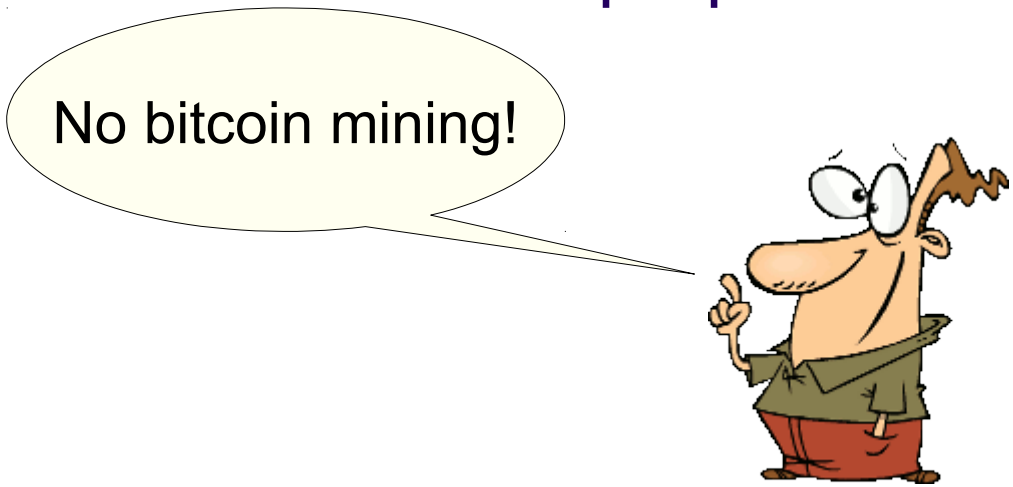
# Privacy

- By default, no privacy in OSG
  - Assume all your files are publicly readable
- If you need privacy, you will have to take explicit measures
  - Both during network transfers, and
  - For files on disk

Not trivial.
Think twice before
putting sensitive information
in OSG.

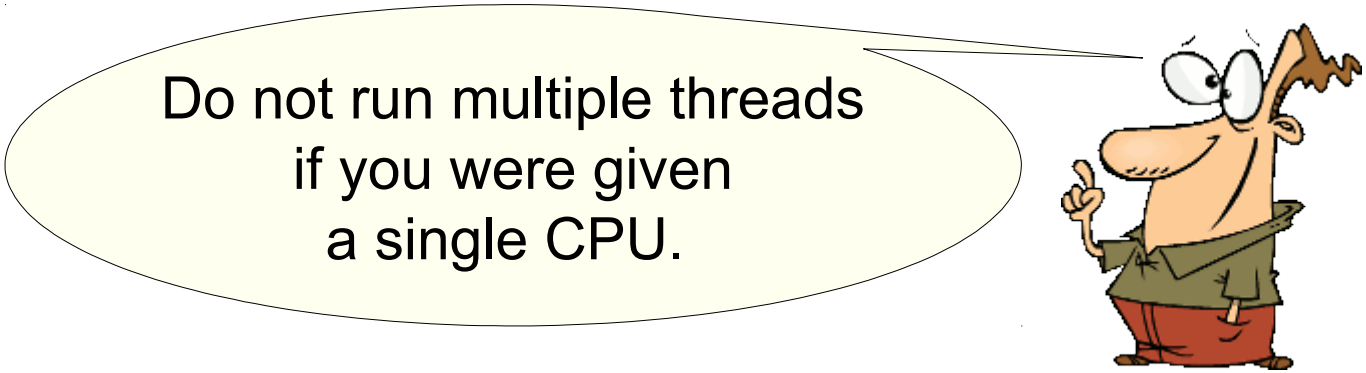
# Acceptable conduct

- Each OSG user is bound by its AUP (Acceptable User Policy)
  - And sites are allowed to have additional rules in place
- In a nutshell
  - Use only for the declared science purpose



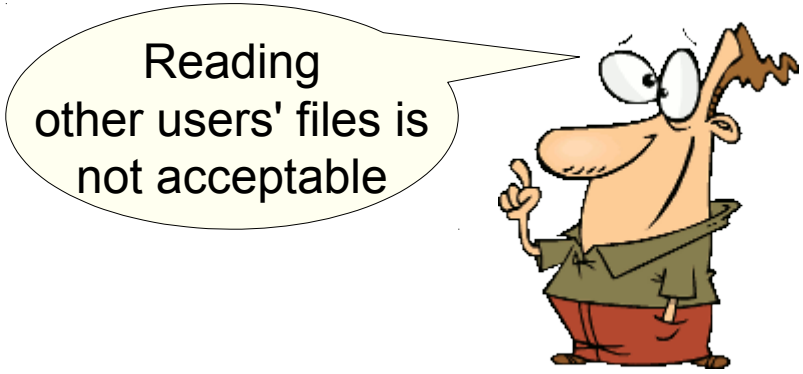
# Acceptable conduct

- Each OSG user is bound by its AUP (Acceptable User Policy)
  - And sites are allowed to have additional rules in place
- In a nutshell
  - Use only for the declared science purpose
  - Do not overload the system



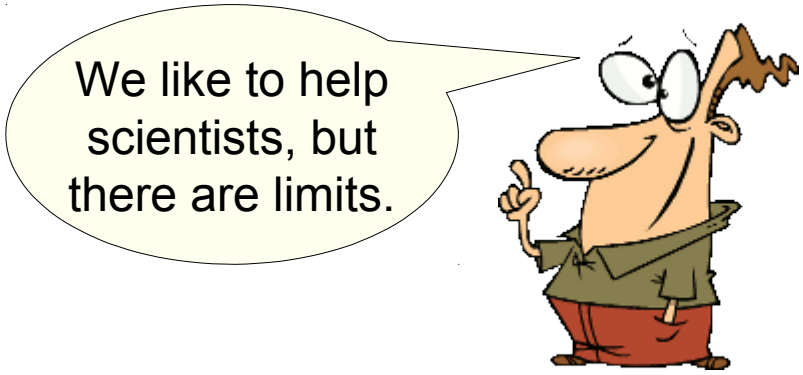
# Acceptable conduct

- Each OSG user is bound by its AUP (Acceptable User Policy)
  - And sites are allowed to have additional rules in place
- In a nutshell
  - Use only for the declared science purpose
  - Do not overload the system
  - Do not attempt to circumvent security
    - Even the one without technical enforcement



# Acceptable conduct

- Each OSG user is bound by its AUP (Acceptable User Policy)
  - And sites are allowed to have additional rules in place
- If you misbehave
  - At the very least, you will get a nasty email
  - You may be banned from using OSG again
  - Police will be called if you break the law



# Questions?

- Questions? Comments?
  - Feel free to ask me questions later:

    Igor Sfiligoi <isfiligoi@ucsd.edu>
- Upcoming sessions
  - Hands on session
  - OSG and BOSCO lectures
  - More hands on

# Security is tricky business

# Copyright statement

- Some images contained in this presentation are the copyrighted property of ToonClipart.
- As such, these images are being used under a license from said entities, and may not be copied or downloaded without explicit permission from ToonClipart.