

Grid Certificate & VOMS

On behalf of JUNO DCI Group





Outline

1. Introduction of the Grid certificate structure,
2. How to apply for a personal CA,
3. How to register VOMS,
4. Create a DIRAC-proxy.



Introduction

The Grid Authentication Model,

- JUNO DCI provides distributed computing and storage resources.
- Every resource has its own local user lists.
- The Grid certificate is a personal certification system for DCI users using distributed resources by mapping Grid users to local user pool.

For Users,

- A **CA certificate**, used for provide your personal information. You need use it to prove you are yourself.

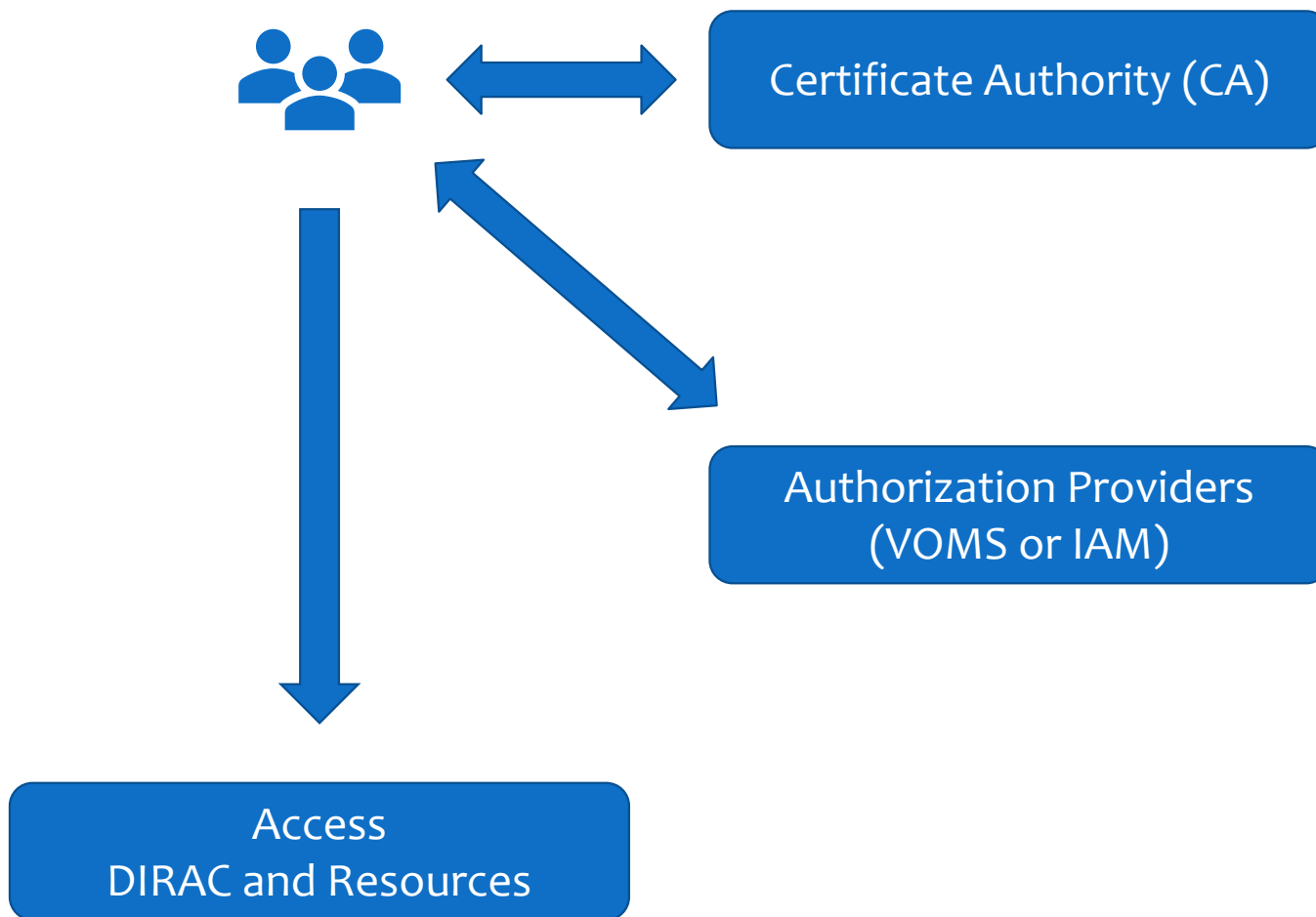
For Resource Sites,

- Sites need to recognized the authenticated users and provided authorized resources.

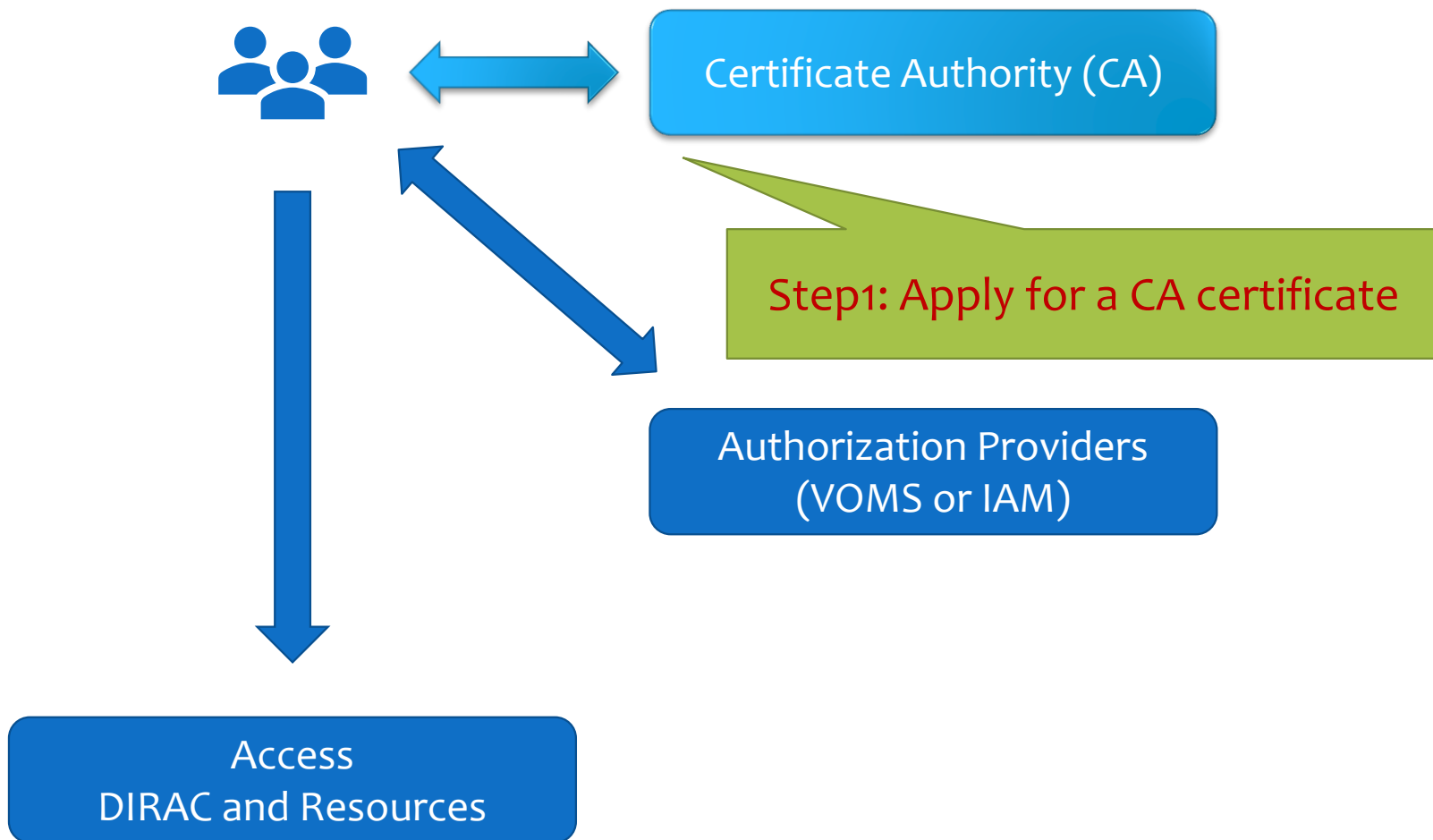
For DCI Service,

- An **Authentication and Authorization Infrastructure (AAI)** need to be build for users and resources sites.

AuthN/AuthZ Model



Step 1





Digital Certificate

A digital certificate (X.509) is normally used as a personal identity for each user.

- Trusted by the organizations in Grid,
- Can be applied from Certificate Authority (CA) in many countries.
- Usually need to provide your personal information and apply on a webpage.

Grid recognized CA examples:

- **IHEP**
 - IHEP Grid Computing Certification Authority ([Link](#))
- **INFN**
 - FAQ ([Link](#))
 - Wiki INFN ([Link](#))
- **CNRS**
 - Request ([Link](#))
- **Germany**
 - CA at Karlsruhe Institute of Technology ([Link](#))
- **Or find other CAs for you at [igtf.net](#).**



CA Certificate

Take **IHEP CA** as an example, details in [link](#),

1. Contact the CA web page and access the request form,
2. Follow instructions to fill application and submit,
3. Receive your personal certificate in **p12 file** format by the link in email.
4. Export the personal certificate to your browser.

About your personal certificate,

- A p12 file composes 2 part,
 - Public key, so called ``cert``,
 - Private key, so called ``key``.
- You need to convert a certificate from p12 to **pem file** format.
 - This will split your certificate by cert and key part.

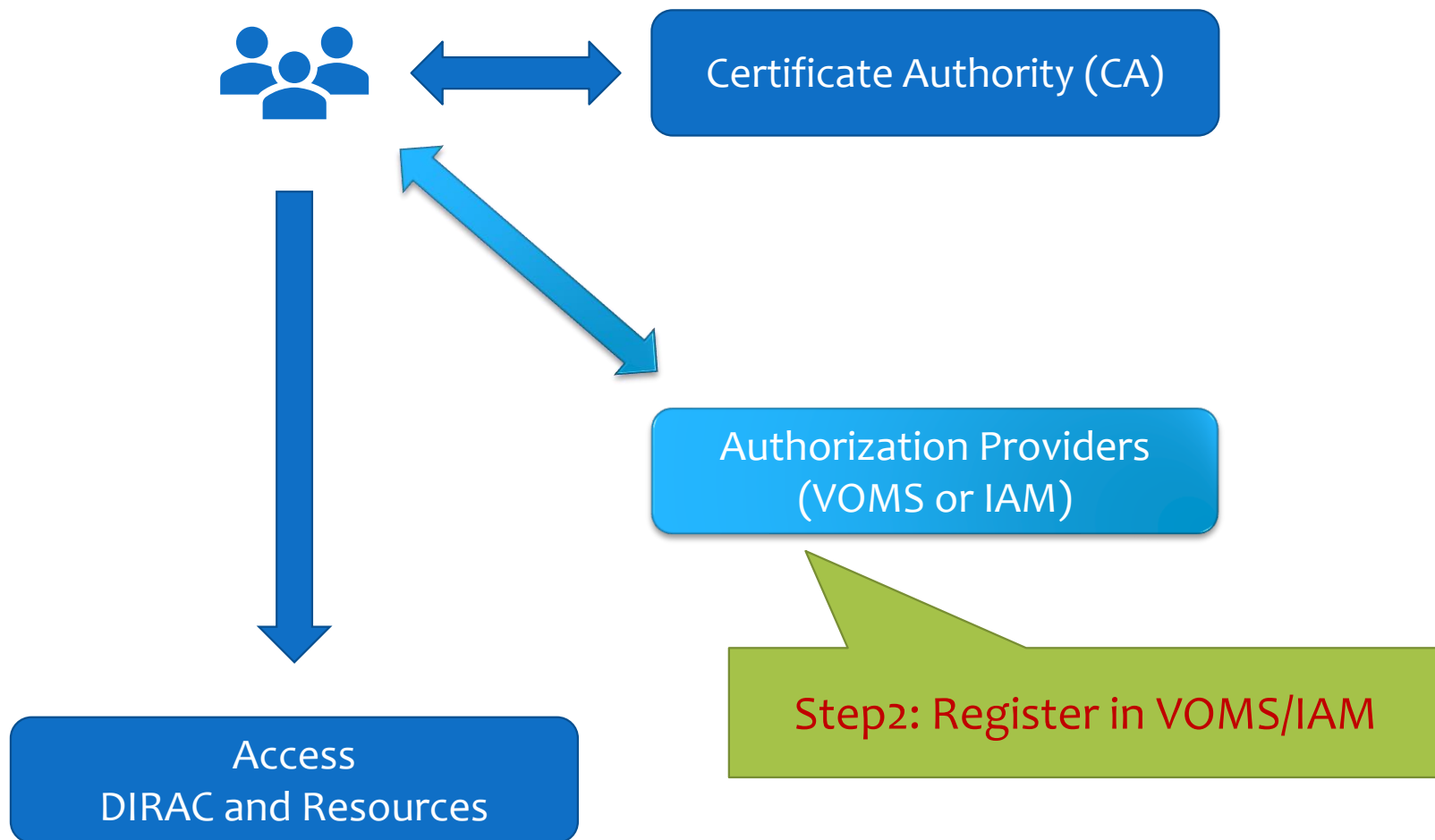


CA Certificate Exercise

Try it:

1. Upload your p12 file to cluster.
2. At cluster, create .globus directory
`mkdir ~/.globus`
3. Extract public key from p12
`openssl pkcs12 -in <certificates>.p12
-clcerts -nokeys
-out ~/.globus/usercert.pem`
4. Extract private key from p12
`openssl pkcs12 -in <certificates>.p12
-nocerts
-out ~/.globus/userkey.pem`
5. Change the access rights for your keys
`chmod 644 ~/.globus/usercert.pem
chmod 400 ~/.globus/userkey.pem`
6. Browse your personal certificate information
`openssl x509 -in ~/.globus/usercert.pem -noout -text`

Step 2



Authorization Providers: VOMS



Virtual Organization (VO),

- A VO is a physical resource provider.
- **JUNO VO** provides DCI resources.

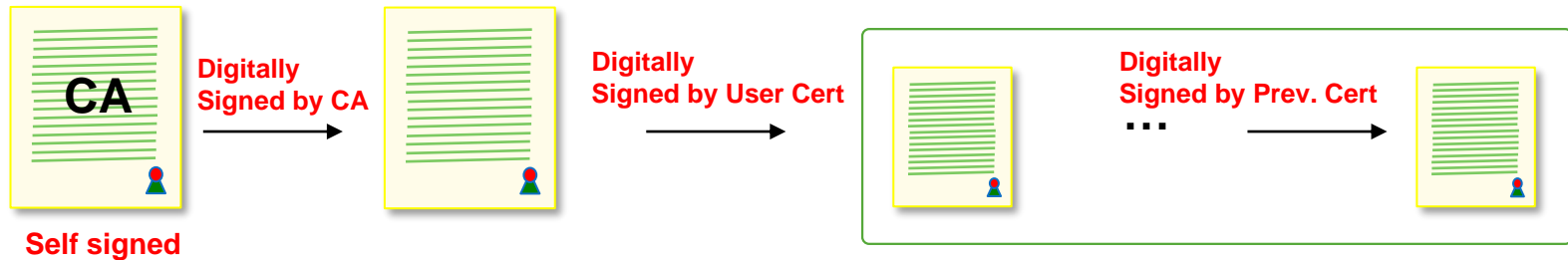
Virtual Organization Membership Services (VOMS),

- Create user groups for VO.
- Create different roles among existing groups.
- Generate VOMS proxy for users to access VO resources.
- Another system, **Identity and Access Management (IAM)**, will replace VOMS as future VO authorization provider.

VOMS Proxy

About VOMS proxy,

- Personal certificate is not directly exposed,
- Most of Grids use temporary certificates (proxies),
- Normal lifetime 12h,
- Proxies are certificates digitally signed by the original certificate or another proxy (delegation),
- Stored proxies may be used to renew other proxies.





VOMS Usage

For a JUNO DCI user,

- **At first time you use DCI, Register yourself in VOMS with your personal certificate at <https://voms.ihep.ac.cn:8443>.**
 1. Select JUNO VO,
 2. Follow instructions to fill application,
 3. Read and allow AUP,
 4. Receive the confirmation email and confirm,
 5. Receive the message email about your accepted application.
- **At each time you use DCI services and resources in cluster, generate VOMS proxy each time.**



VOMS Exercise

Try it:

1. Look at your VOMS personal information at [VOMS user home](#).

2. At cluster, generate VOMS proxy

```
voms-proxy-init --voms juno
```

3. Get your proxy info by

```
voms-proxy-info --all
```

4. Check your proxy credential by

```
openssl x509 -in /tmp/x509up_u$(id -u) -noout -text
```

5. For IHEP EOS user,

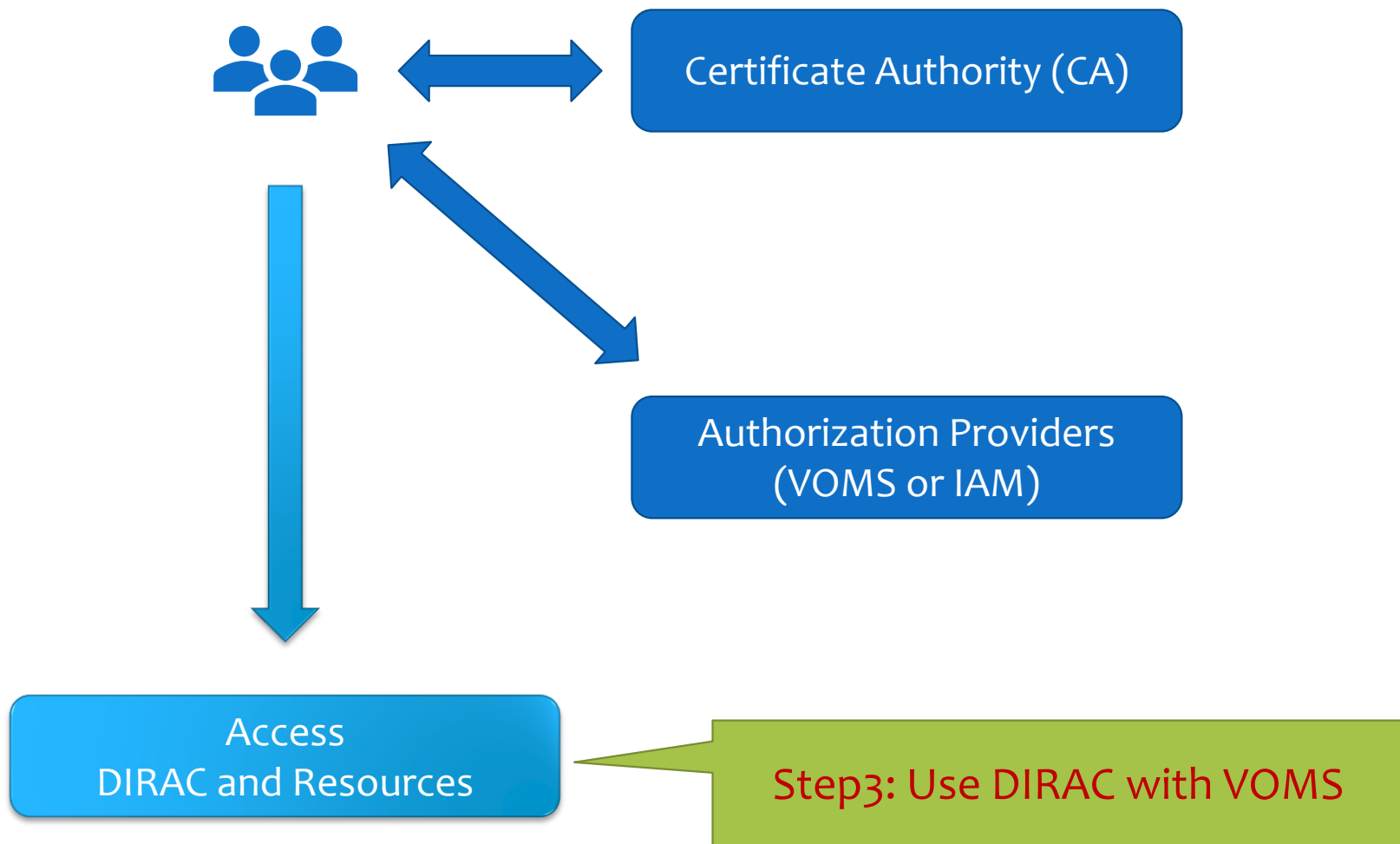
- The EOS identification priority is **Grid cert > local user**, so when you set the globus environment, `eos` command will inform you to type in your Grid password.

```
230207 18:16:02 25149 cryptoss1_X509CreateProxy: Your identity:  
/C=CN/O=HEP/O=IHEP/OU=CC/CN=Xuantong Zhang
```

```
Enter PEM pass phrase:
```

- If you do not want to use grid user identity just tape Enter without input password.
- Or you can rename your Grid certs by `mv ~/.globus/ ~/.globus.juno/` to always use local user identity.`

Step 3





DIRAC Proxy

DIRAC also uses VOMS proxy to identify users,

- Both for login DIRAC and use DIRAC working on resources.
- DIRAC will synchronize your user information from VOMS to DIRAC registry system.

Access DIRAC,

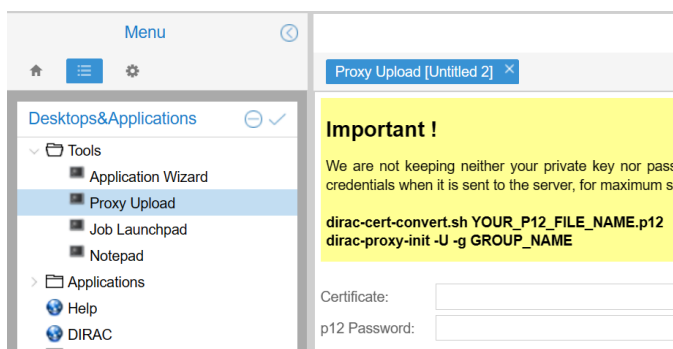
- On webpage, use your personal certificate in browser.
- At cluster, generate DIRAC proxy, which is almost same method as VOMS proxy.

A screenshot of a web portal configuration interface. At the top, there is a "Menu" header with a back arrow. Below the header are navigation icons: a home icon, a hamburger menu icon, and a gear icon. The main content area is titled "Desktops&Applications" and includes a "Settings" section. Under "Settings", there is a "Portal configuration" section with four dropdown menus: "User" (selected: xzhang), "Group" (selected: juno_user), "Setup" (selected: CAS_Production), and "Theme" (selected: Crisp). Below this is an "Active desktop configuration" section with a "Name" field set to "None" and an "Automatic tab change" button set to "Disable".

DIRAC Proxy Exercise

Try it:

1. Access [DIRAC webpage](#) with your personal certificate.
2. Upload your own proxy to DIRAC.



3. At cluster, generate your DIRAC proxy

```
source /cvmfs/dcomputing.ihep.ac.cn/dirac/IHEPDIRAC/bashrc  
dirac-proxy-init -g juno_user
```
4. Check your DIRAC proxy

```
dirac-proxy-info
```


Thank you!

