

Connecting with SSH

<https://indico.cism.ucl.ac.be/event/181/timetable/#day-2026-10-07>





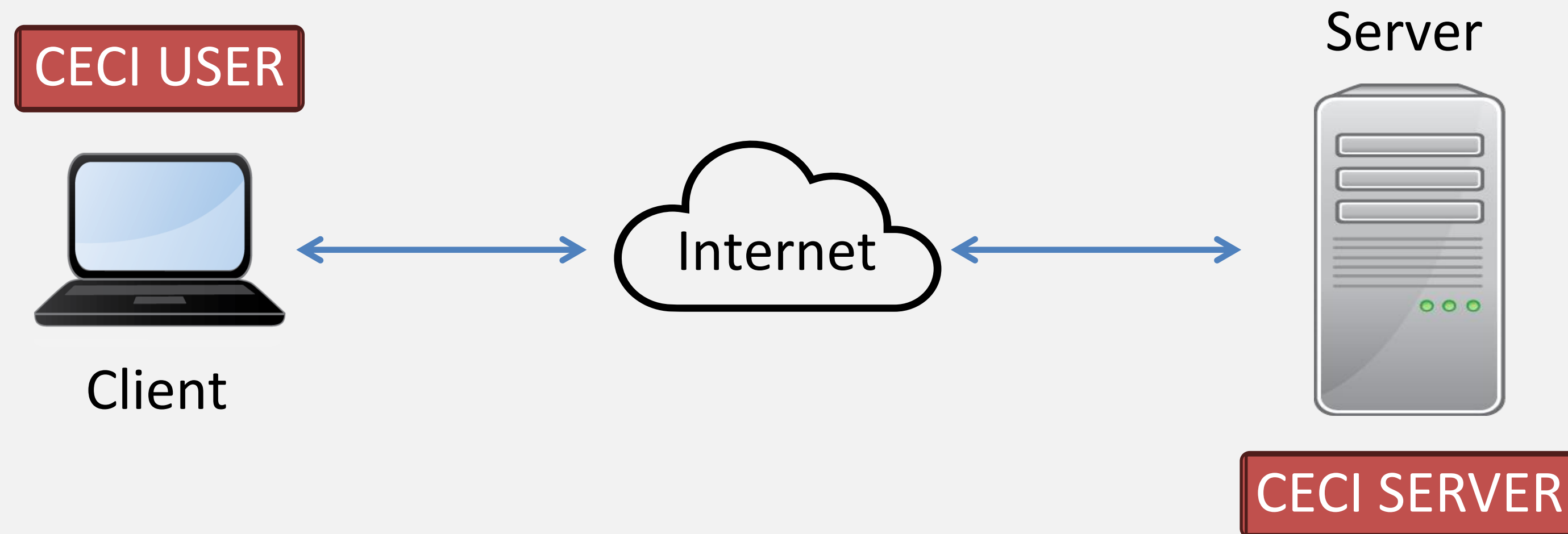
Part 1

Context

SSH

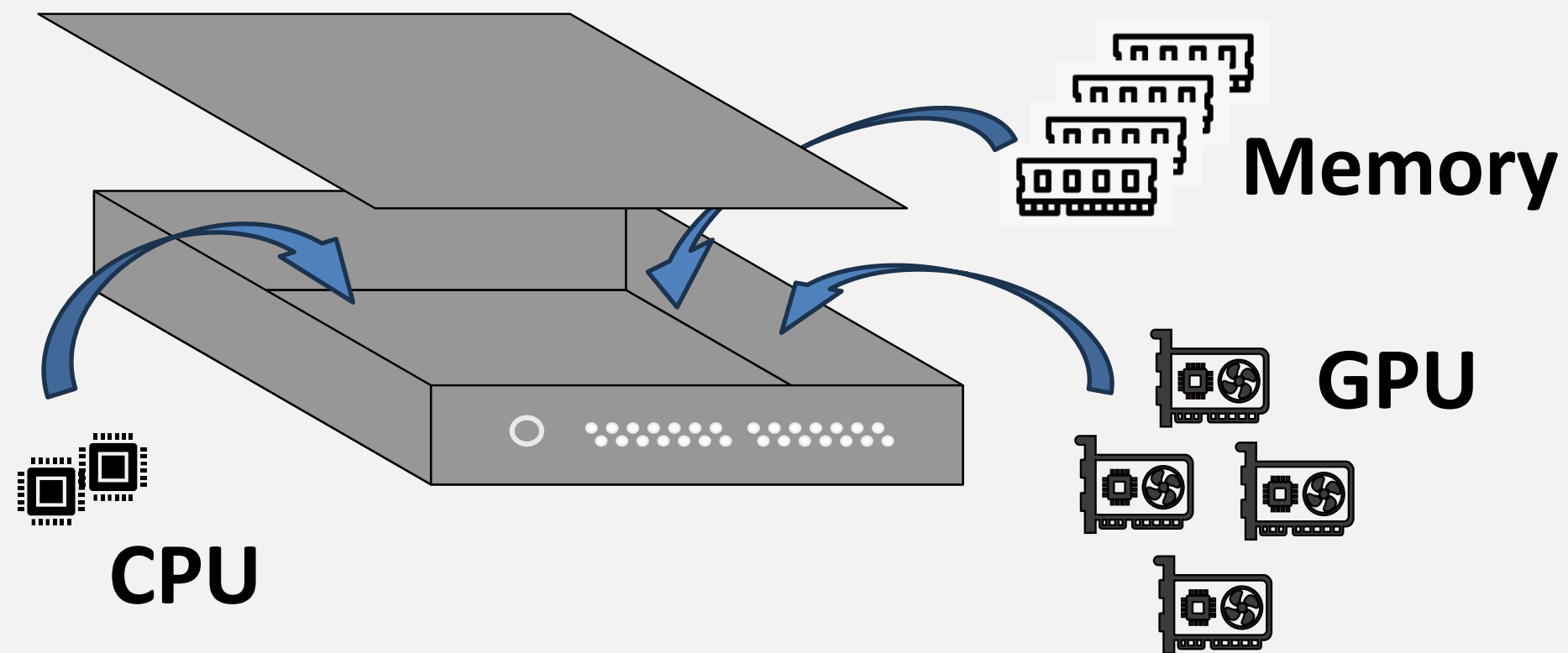
Secure Shell protocol

Client server model

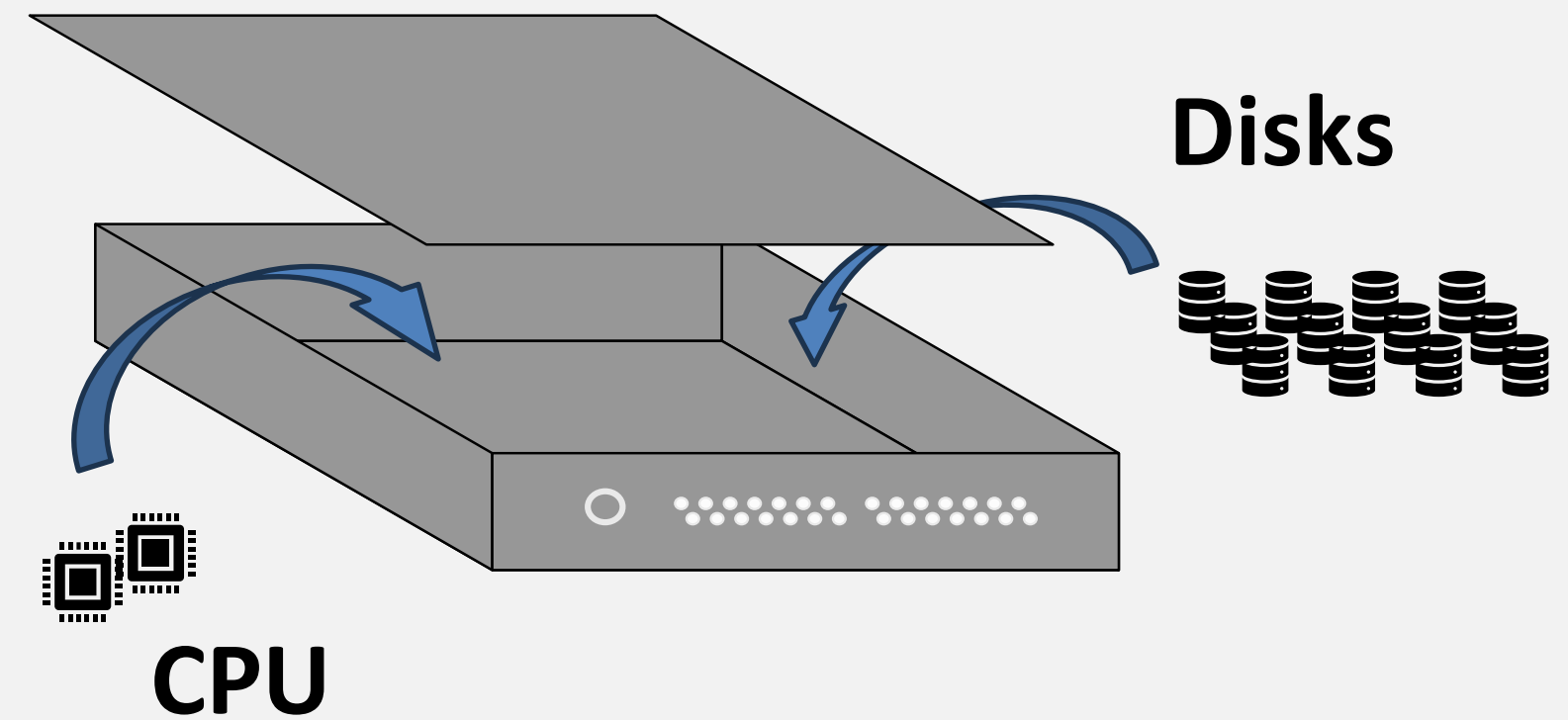


Context

Compute nodes for calculation



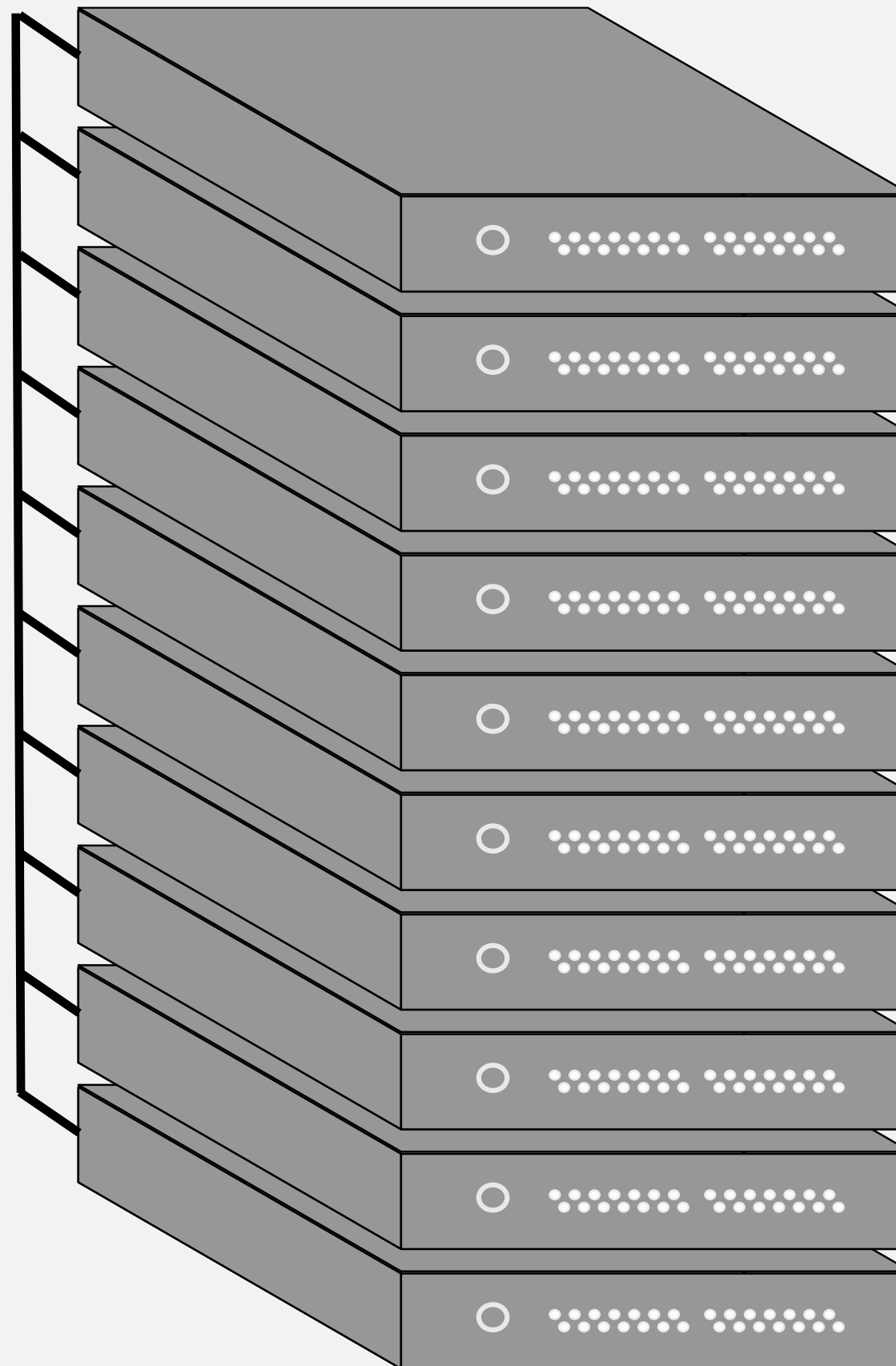
Storage nodes to save data files



Context

Cluster: stack of nodes

**Fast Private
network**



Context

Cluster: stack of nodes



**Fast Private
network**



Context

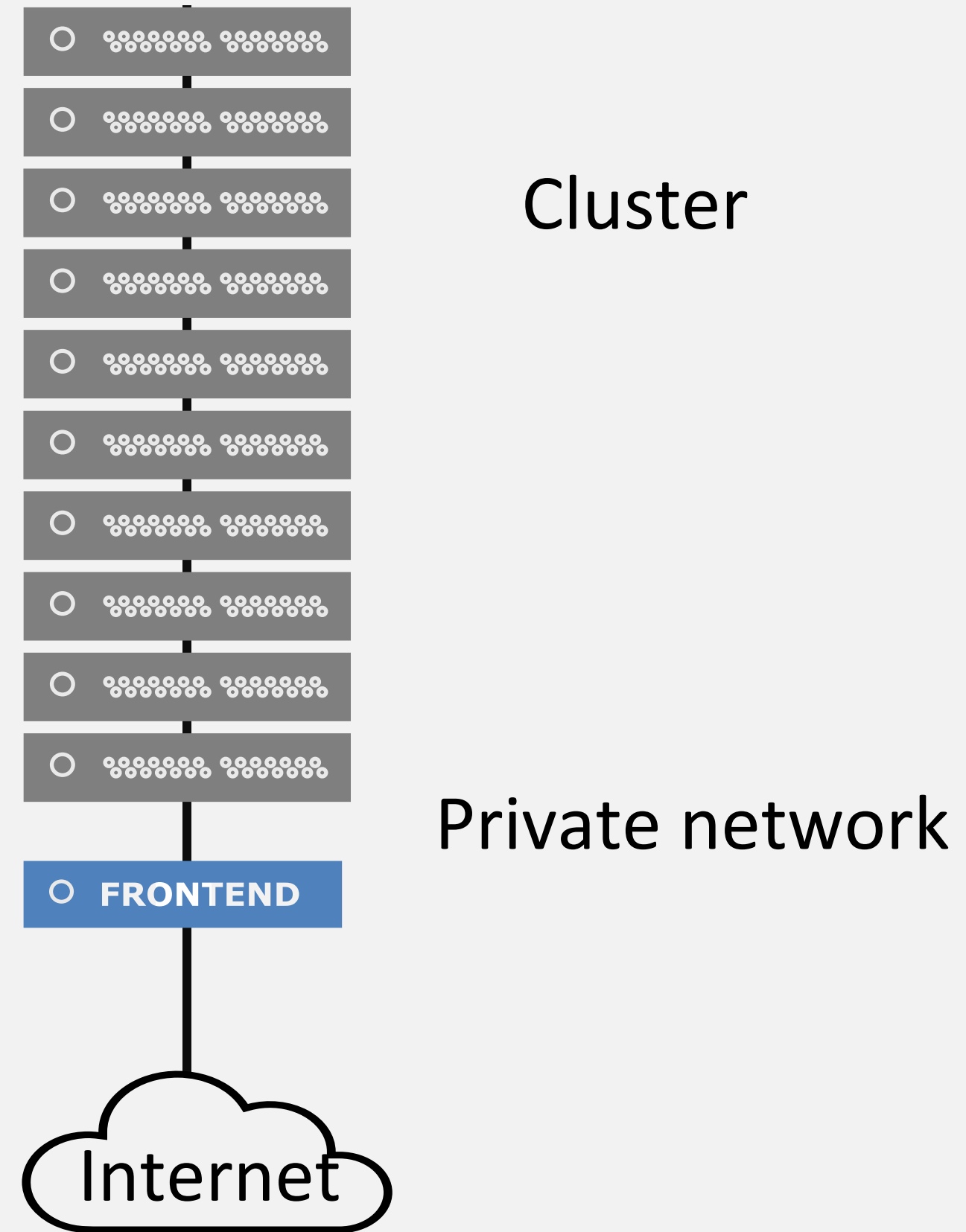
Frontend

You need to connect with SSH to the **frontend** to :

- **submit jobs** to the compute nodes (**SLURM**)
- **access** your results
- **edit** your files
- **compile (use debug partition)**
- **transfer** your data

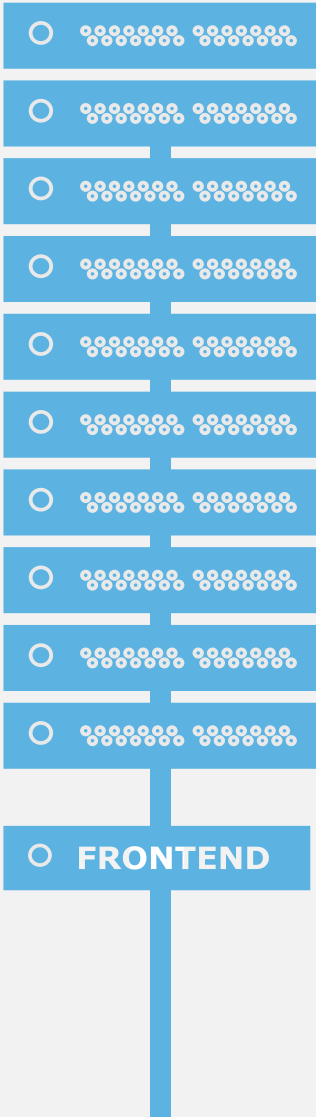


Do not run heavy jobs on the frontend

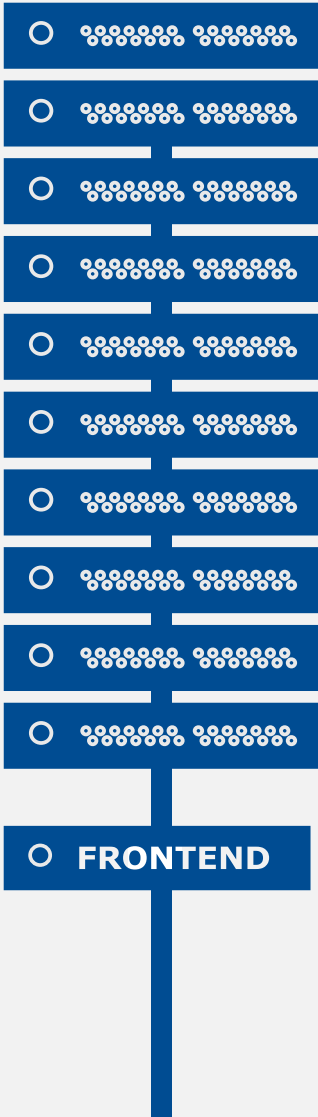


Context

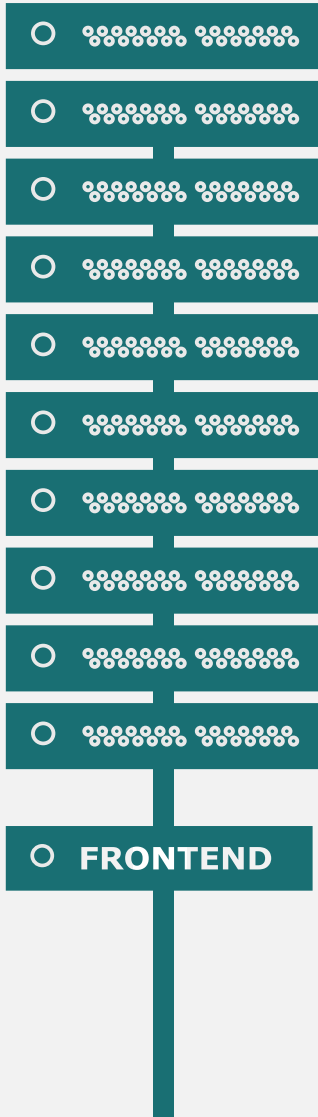
Lemaitre 4



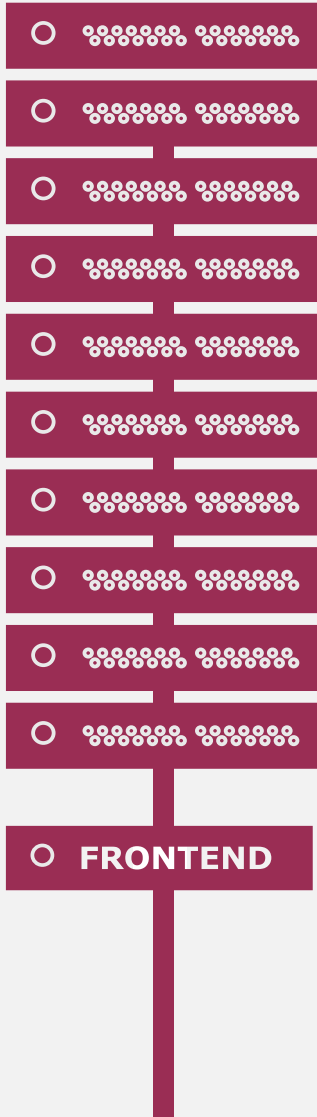
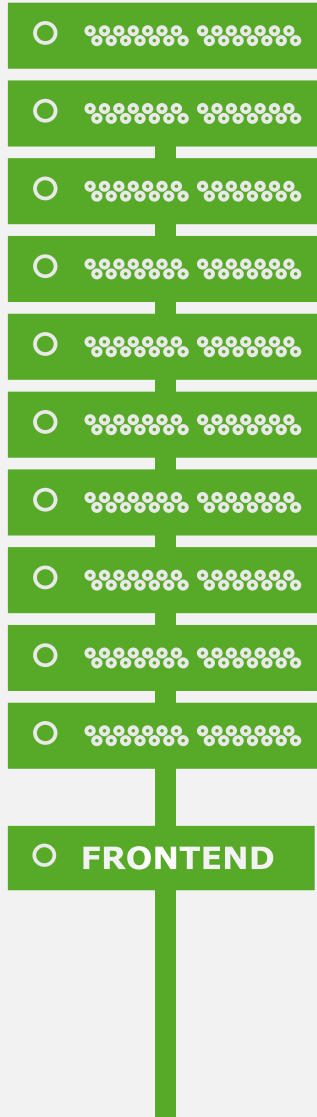
Lyra



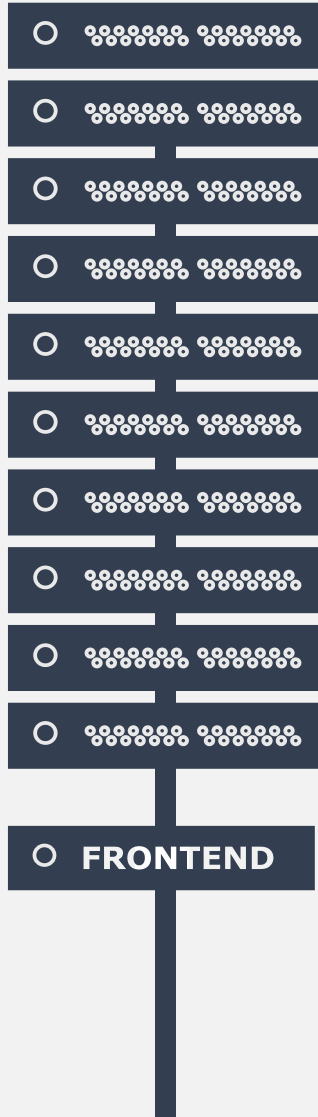
Nic6



Hercules 2 Dragon 2/3



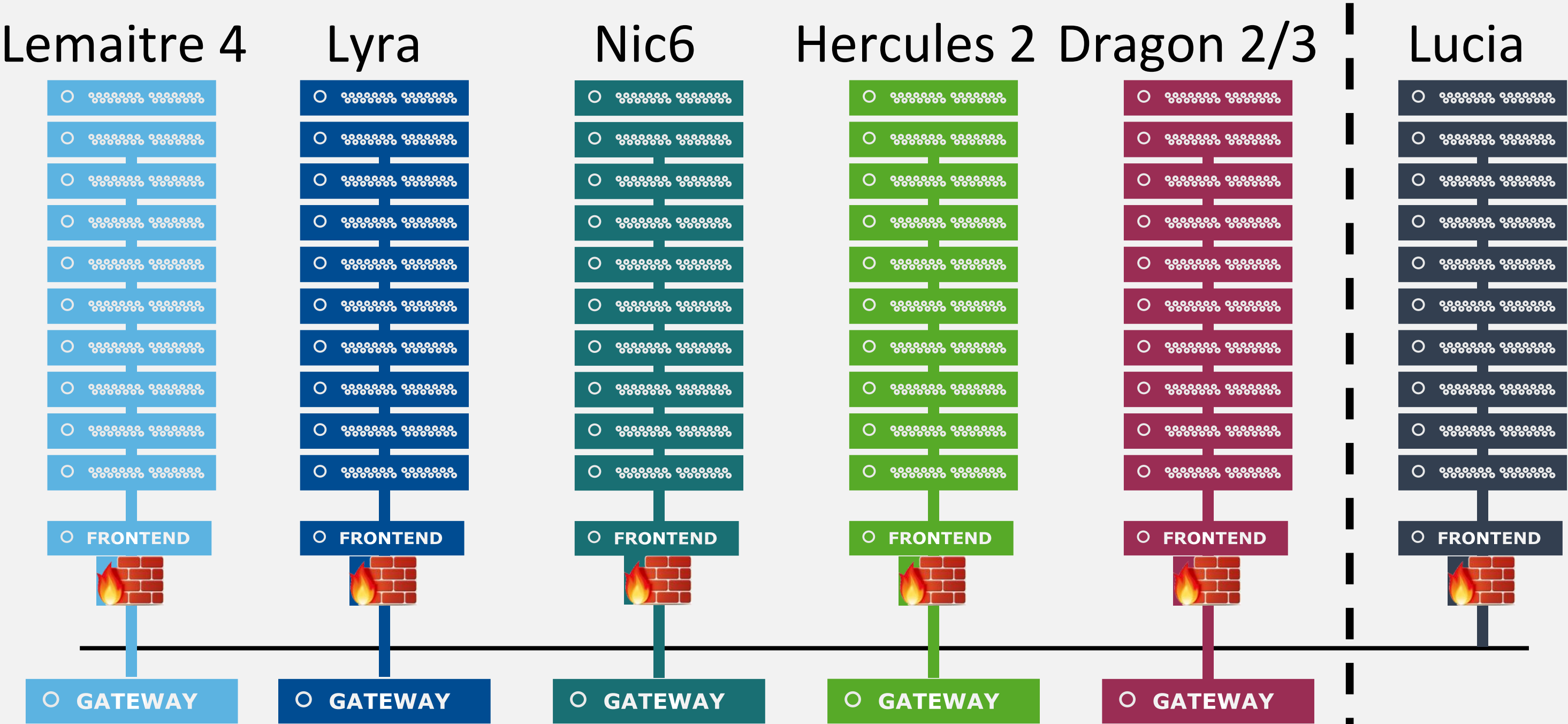
Lucia



6 CÉCI
Tier 2 clusters

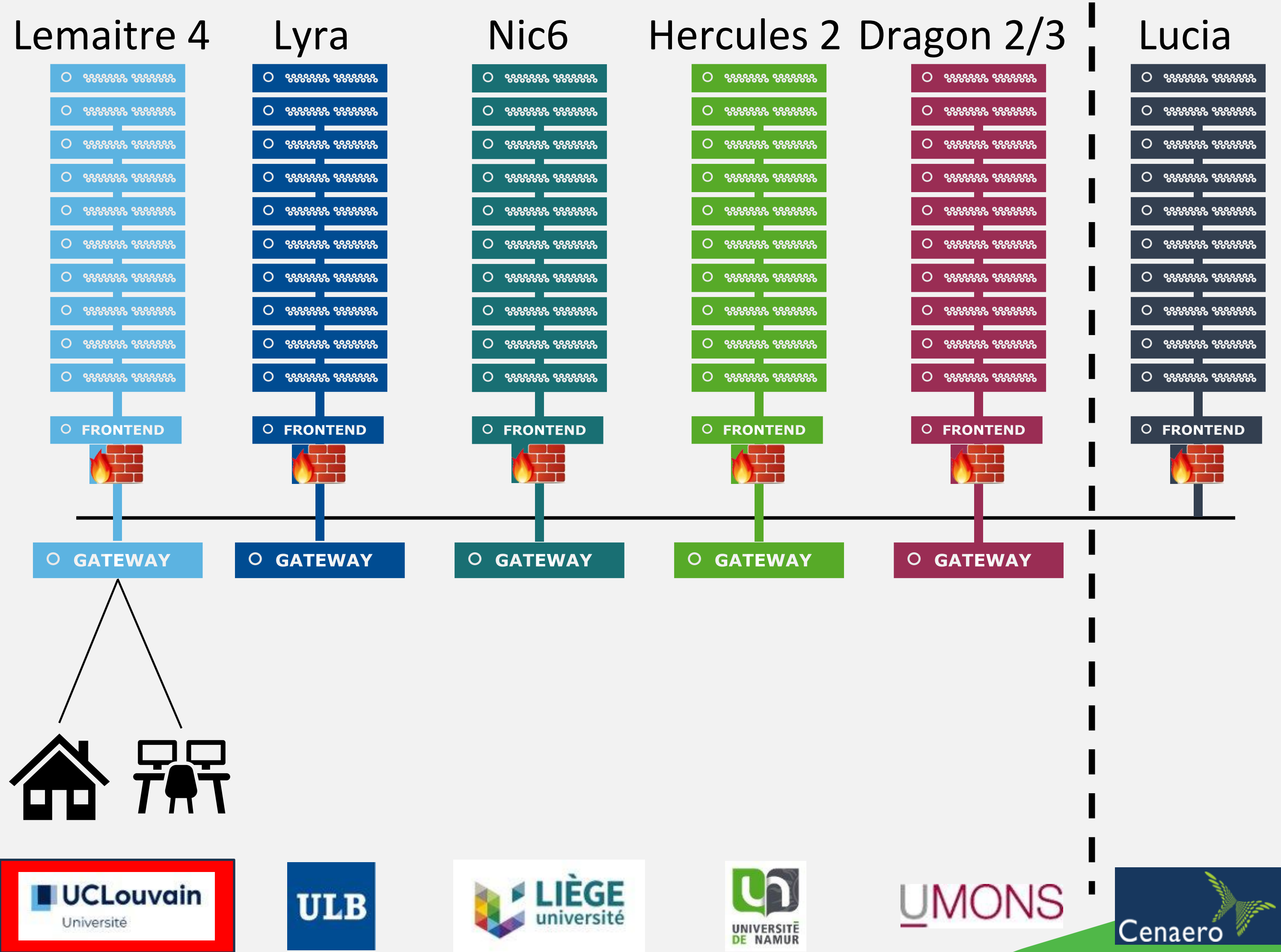
1 Cenaero
Tier 1 cluster

Context

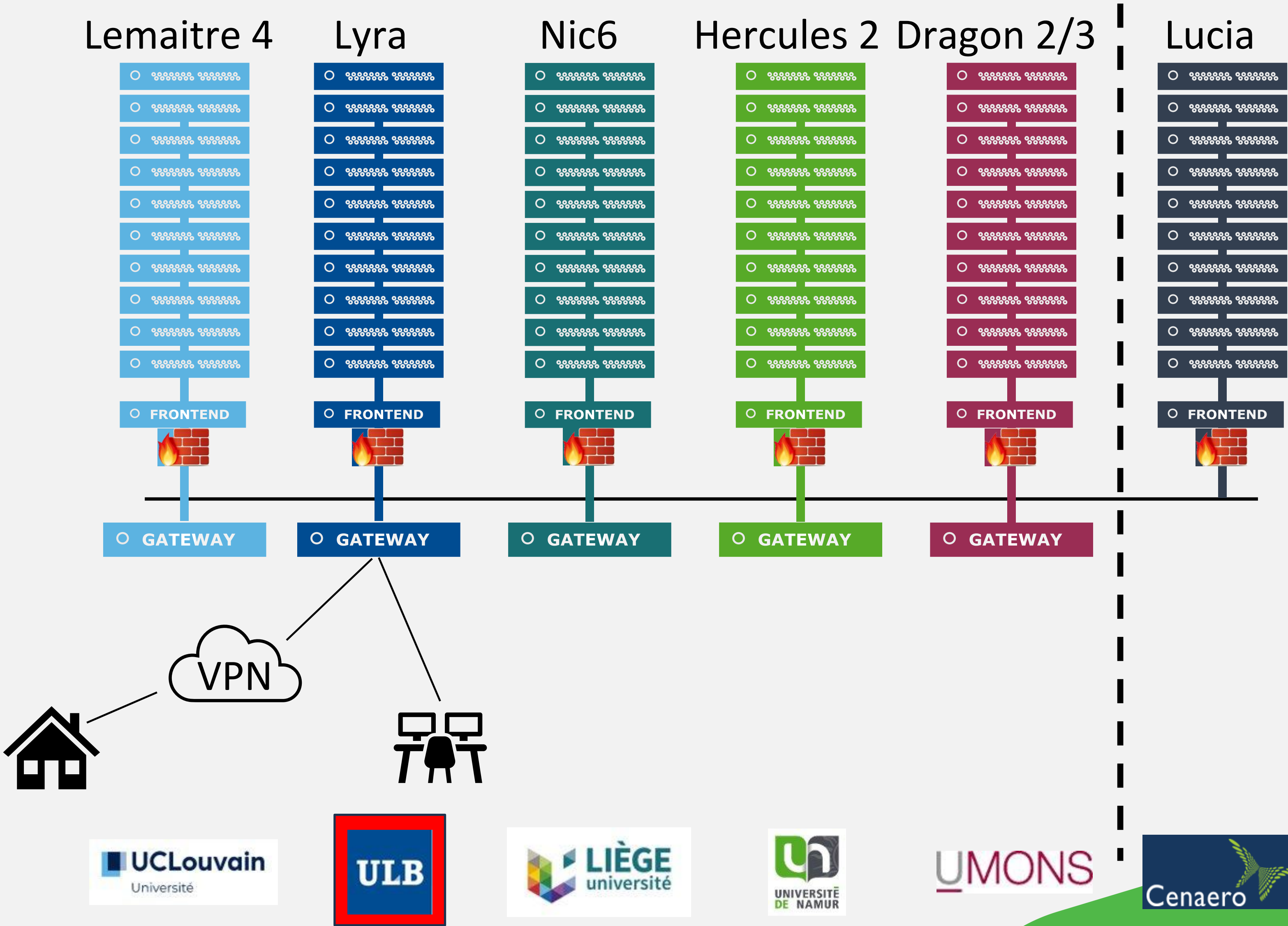


Frontend Firewall rules
Access only through a Gateway

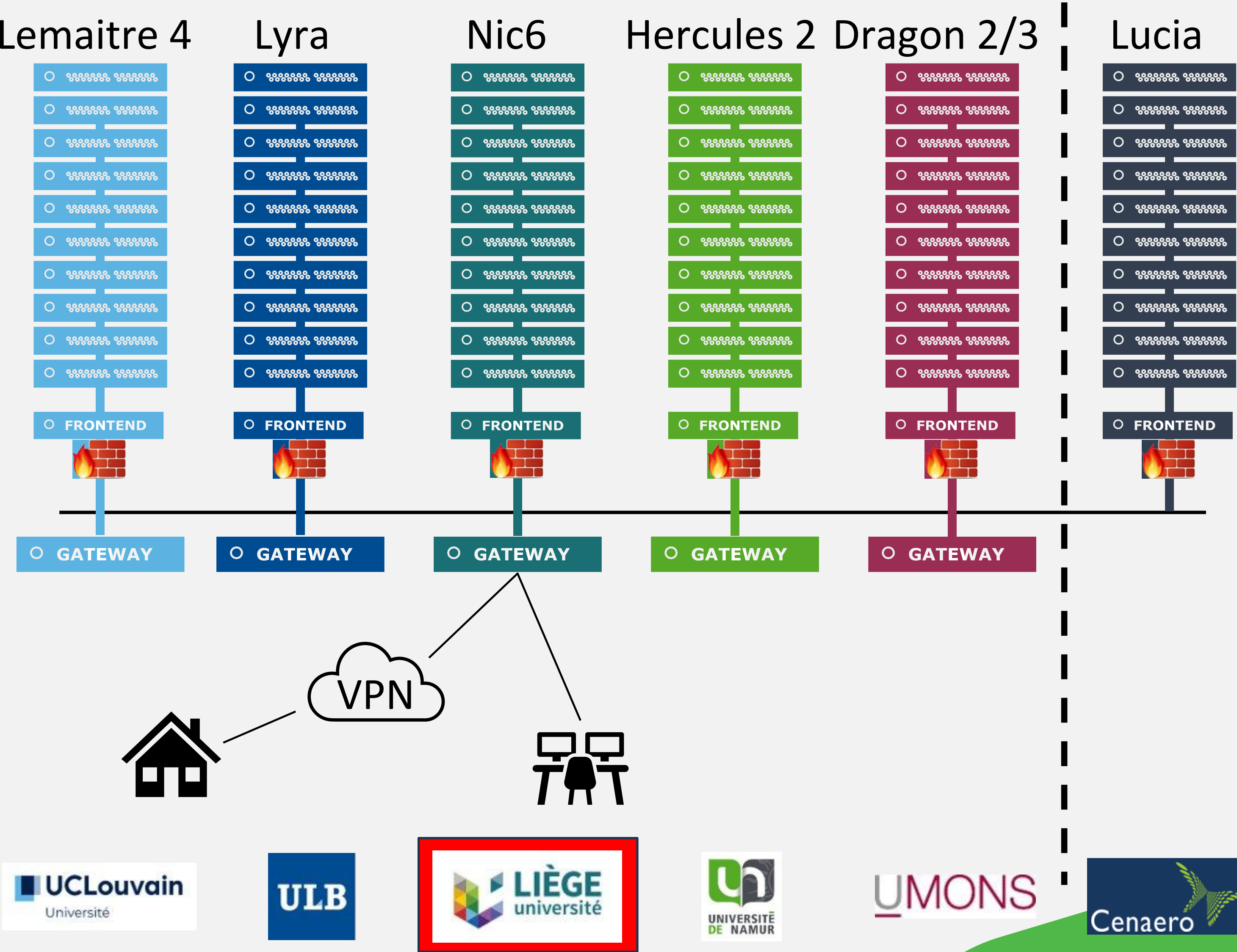
Context



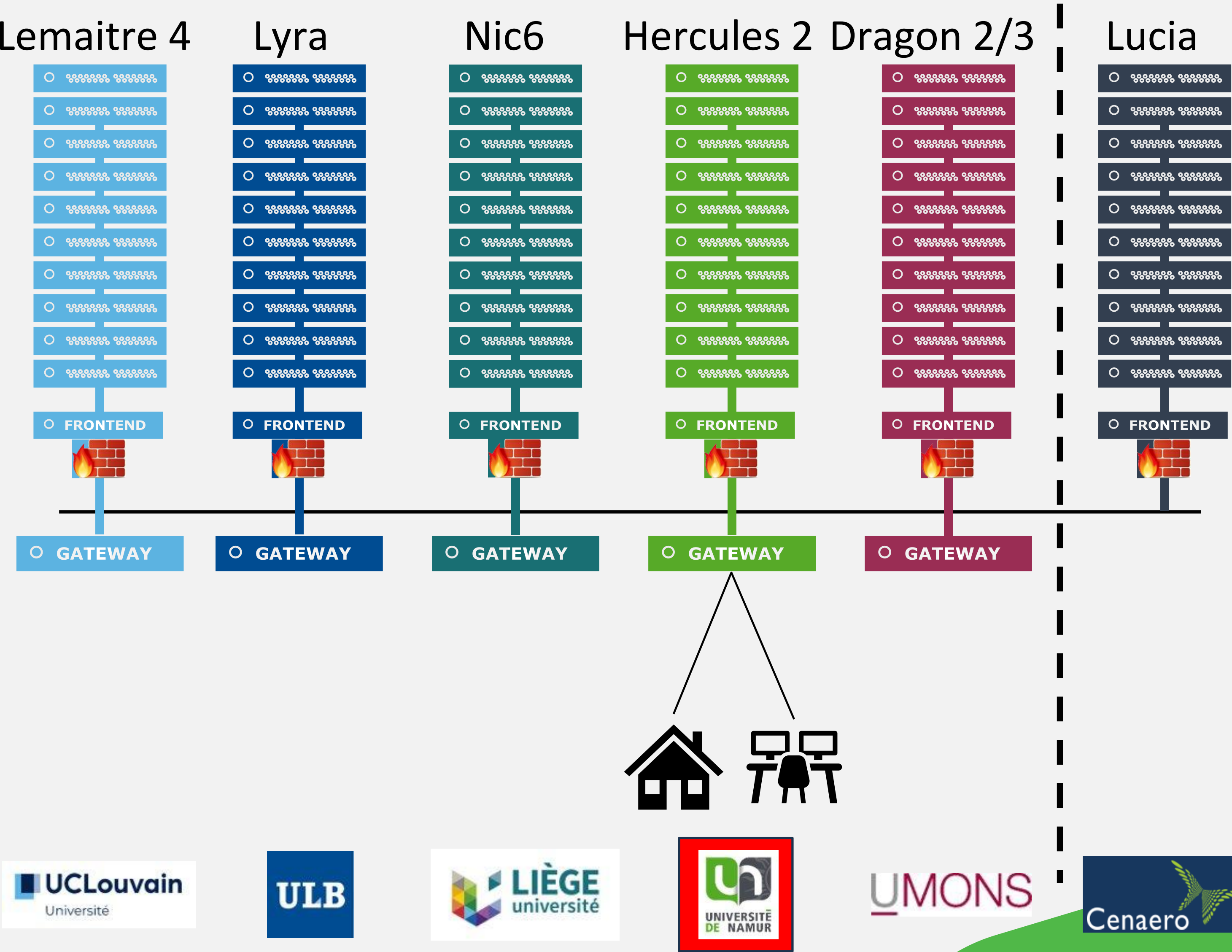
Context



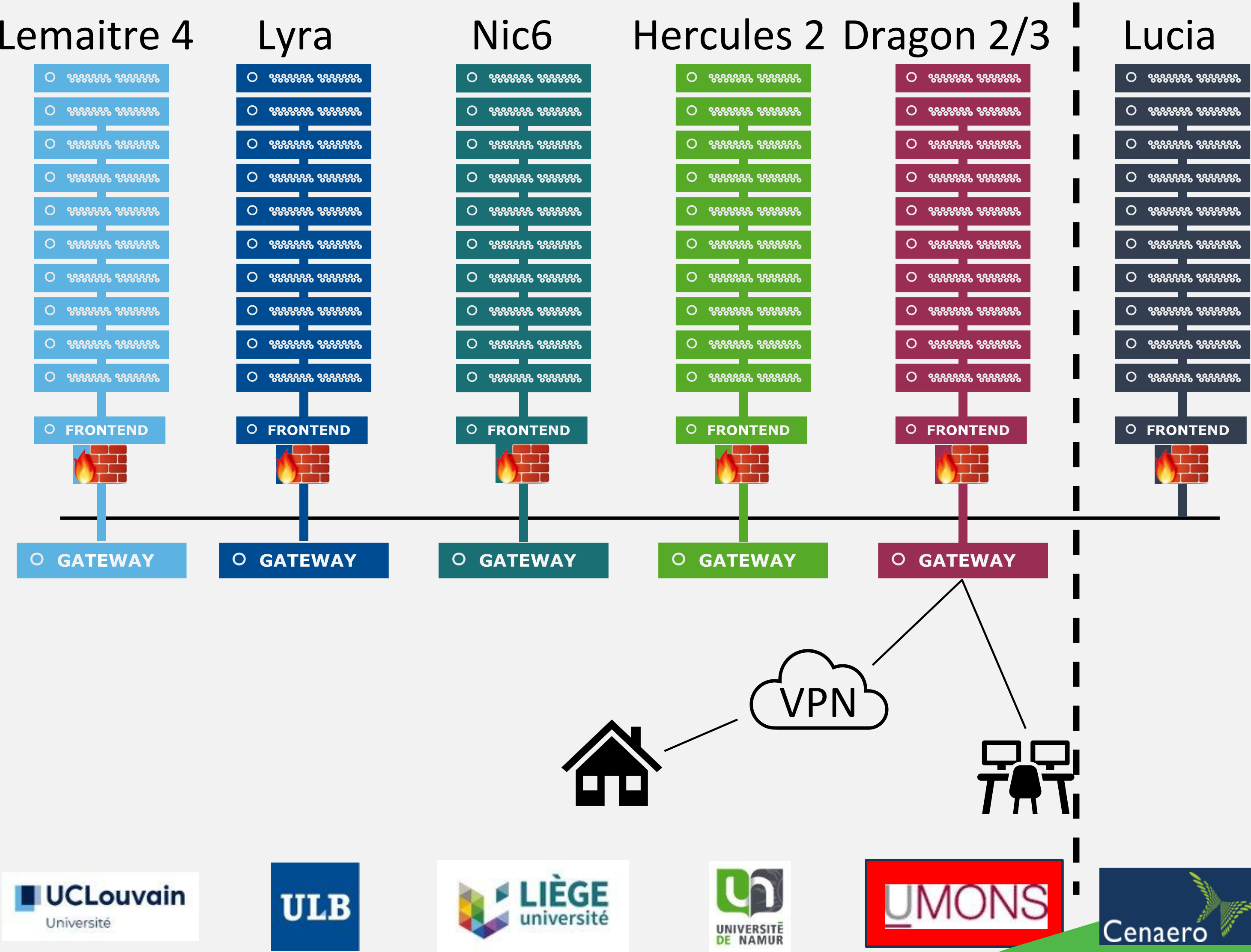
Context



Context



Context





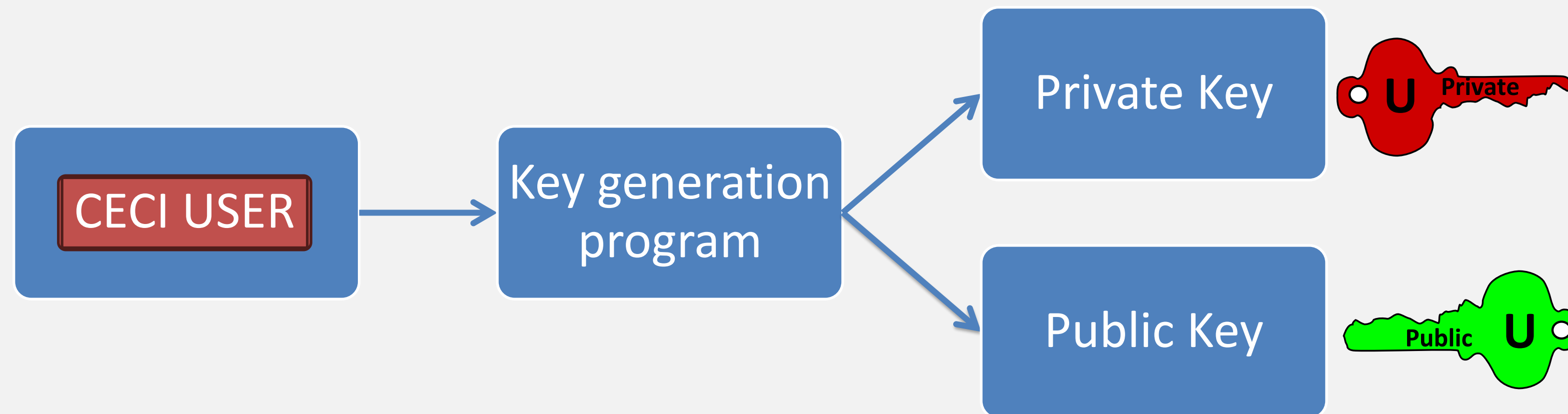
Part 2

Secure Shell protocol

SSH

Secure Shell protocol

Public-key cryptography for **authentication**

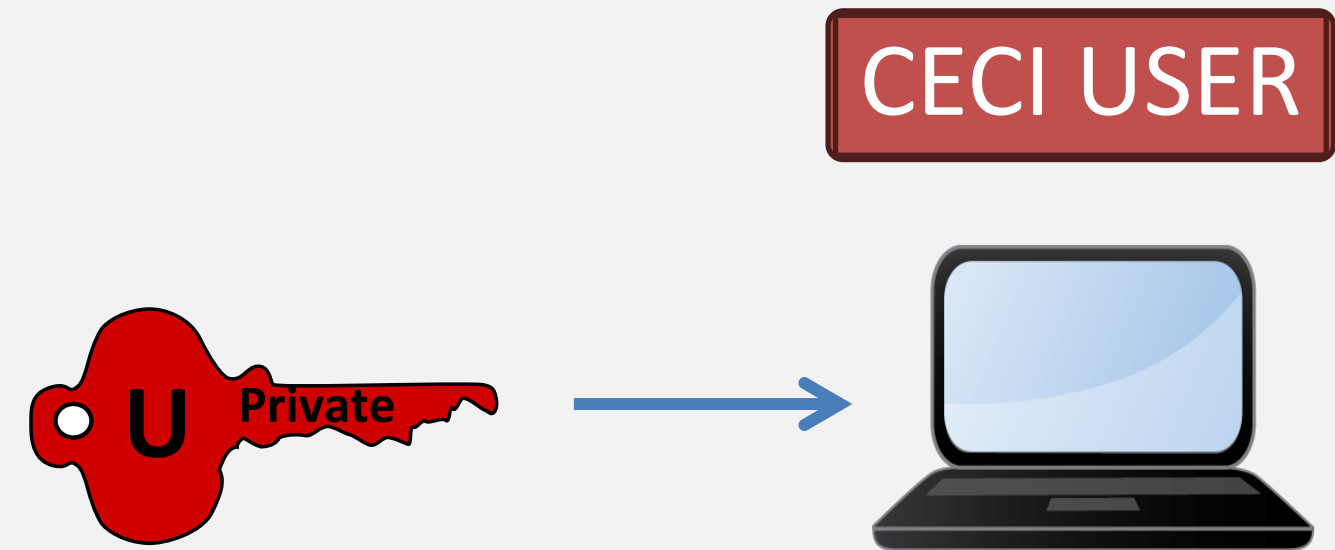


Secure Shell protocol

Public-key cryptography for **authentication**

Private key

- Proves your identity
- File named **id_<algorithm>** (e.g., id_rsa.cecil)
- Encrypted with a passphrase for protection
- Used to sign messages or documents



Keep it secure:

- Store in a safe location
- Set correct file permissions

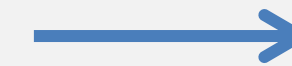
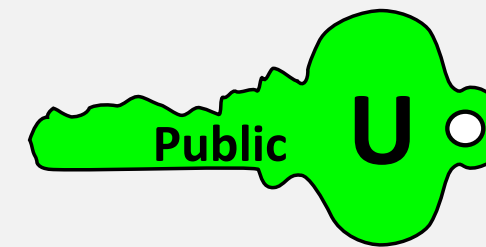
```
-----BEGIN OPENSSH PRIVATE KEY-----
b3B1bnNzaC1rZXktdjEAAAACMFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABAw9XHEY5
n25/tBVF33WGAgAAAAEAAAAEAAAIXAAAAB3NzaC1yc2EAAAADAQABAAQK3dJeBAxne
X2wbh3hr51jRpEVbNJAuoav+DApUN4pvc2LVX+bSdork05Q8W0smmfD5KRWta0zHnoMLQ
oodyVPXbQ0U3n7PKbWo4e6E6KDqr6hiADz/7k6CxuFENKaqJPEHQ+r8L2uI8hbi39jDW1g
...
qZArZOS60MmQ7whVMdGLufJ0E3EWr1ooU4RgdbJLnaSAVjDZXsImWjHHjJsWHKqKM1ScXU
NkdG005Lp0K3uFBvU+H4F+DYnZTBIOa8VL3JNZy+MbDRUKwpreyy8gXqo9UvfV20HwjOr
NkE7jigKF+UJ9cceZs8XqNdmE=
-----END OPENSSH PRIVATE KEY-----
```

Secure Shell protocol

Public-key cryptography for **authentication**

Public key

- Mathematically linked to the private key
- File named **id_<algorithm>.pub** (e.g., id_rsa.cecil.pub)
- Installed on servers you want to access
- Used to verify your identity
- Can also encrypt data (decryptable only with the private key)



CECI SERVER

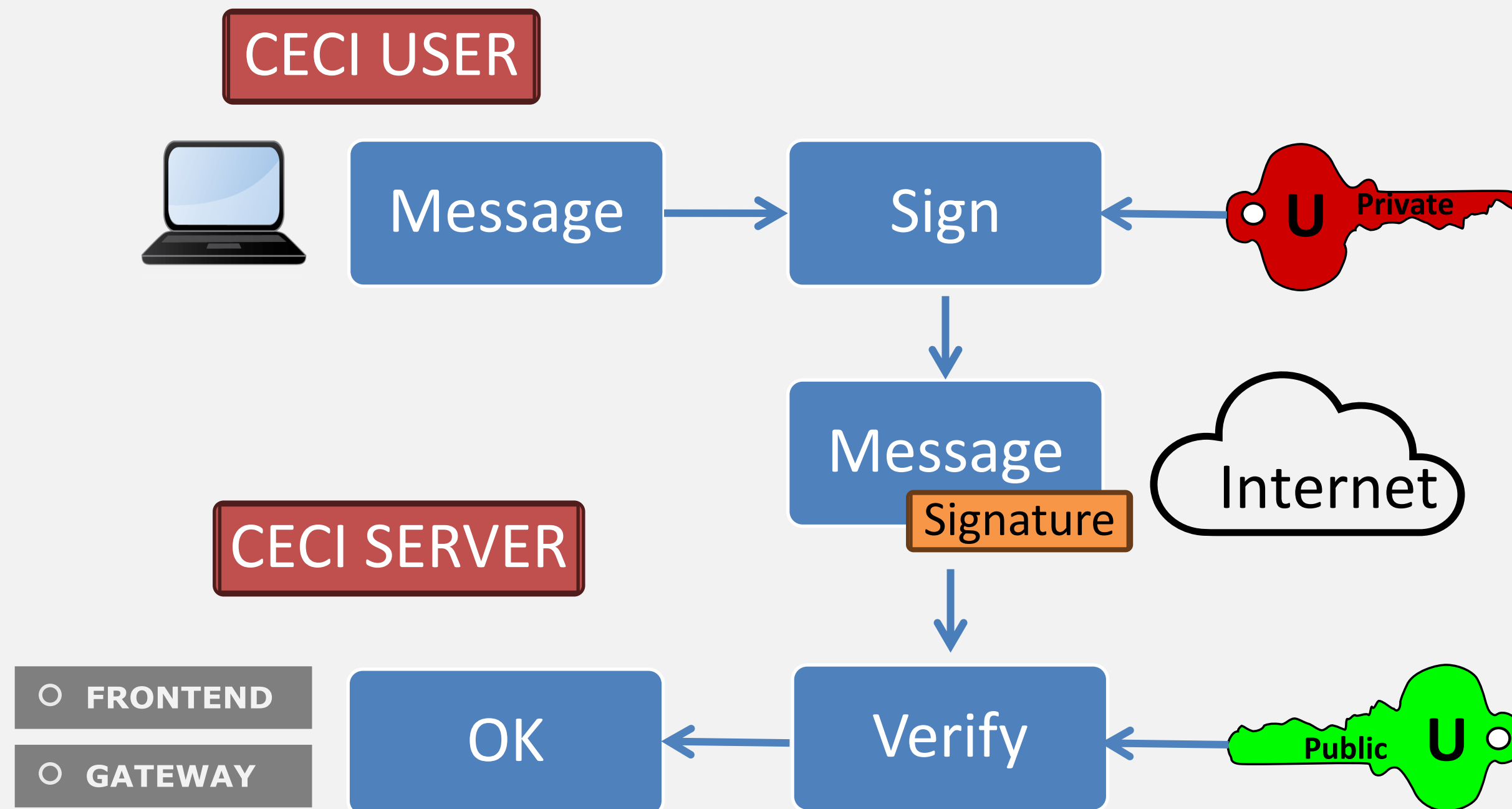
○ FRONTEND

○ GATEWAY

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQK3dJeBAxneX2wbh3hr51jRpEVbNJAuoav+  
DApUN4pvc2LVX+bSdork05Q8W0smmfD5KRWTaOzHnoMLQodyVPXbQ0U3n7PKbWo4e  
...  
ZGCTS/jY2i9QFUIp7+I1p9vqtNSV0uIytwFfL7tU= relog@ceci-relog.segi.ulg.ac.be
```

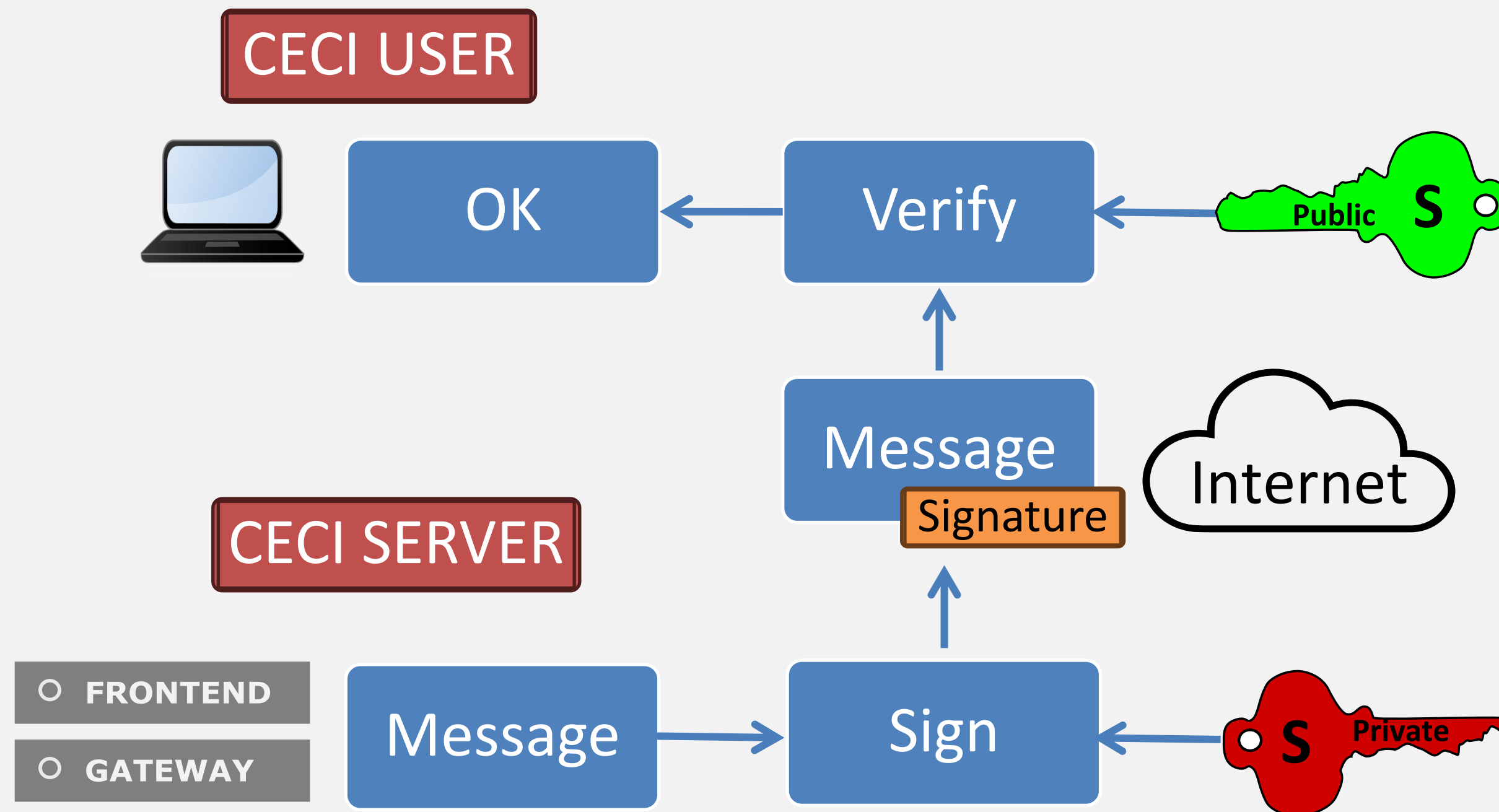
Secure Shell protocol

Public-key cryptography for **authentication**



Secure Shell protocol

Public-key cryptography for **authentication**



SSH

Secure Shell protocol

Encrypted communication and data transfer

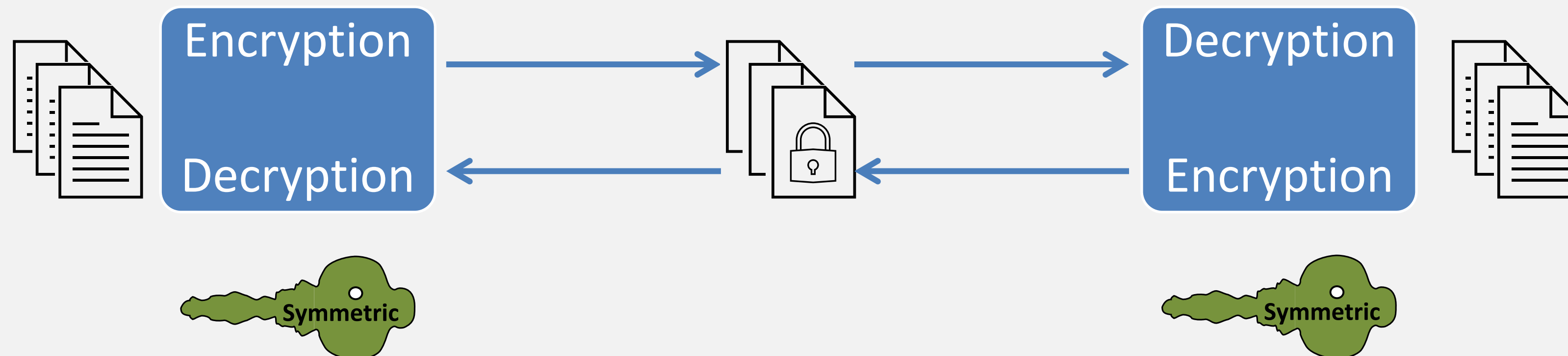
CECI USER

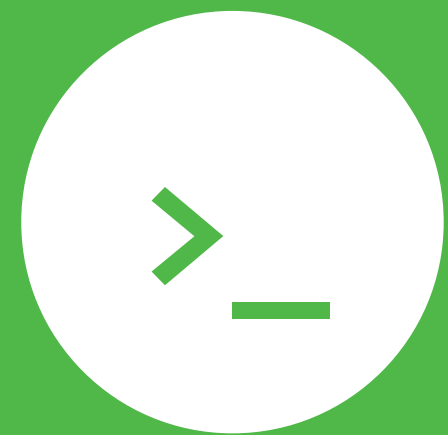


CECI SERVER

○ FRONTEND

○ GATEWAY





Part 3

CÉCI Account

Create an account and get your private key

Go to

<https://www.cec-hpc.be>

I want to...

- [create an account](#)
- [renew my account](#)
- [join an existing project](#)

create an account

My email address:

@uclouvain.be

[Send](#)

Create an account and get your private key

Click on the link sent to you by email and fill-in the form.

**Supervisor must have
a permanent academic
or scientific position**



1. Enter your information

First Name

Last Name

Email of Supervising Professor

 @unamur.be ▼

You are not allowed to give your own email address. We need a secondary contact. If you are the supervisor, please provide the email address of a trusted colleague.

2. Choose a credential

Login

The login must be between 4 and 8 characters long, can only contain lowercase letters, and must reflect your last name.

Passphrase

The passphrase must be at least 8 characters long and contain at least one figure, one uppercase letter and one special character

Please repeat Passphrase

3. Pick your affiliation

You need to choose your primary affiliation as recorded in the official directory of your university, down to the third level. Should an option be missing, please [contact us](#).

University

Université catholique de Louvain ➤

Département

Département des Sciences ➤

Unité / Laboratoire

Groupe de recherche sur les

Create an account and get your private key

Click on the link sent to you by email and fill-in the form.

UNamur users
Use your UNamur eid

1. Enter your information

First Name

Last Name

Email of Supervising Professor

 @unamur.be ▼

You are not allowed to give your own email address. We need a secondary contact. If you are the supervisor, please provide the email address of a trusted colleague.

2. Choose a credential

Login

The login must be between 4 and 8 characters long, can only contain lowercase letters, and must reflect your last name.

Passphrase

The passphrase must be at least 8 characters long and contain at least one figure, one uppercase letter and one special character

Please repeat Passphrase

3. Pick your affiliation

You need to choose your primary affiliation as recorded in the official directory of your university, down to the third level.
Should an option be missing, please [contact us](#).

University

Université catholique de Louvain ➔

Département

Département des Sciences ➔

Unité / Laboratoire

Groupe de recherche sur les

**Use a strong
passphrase to
encrypt your key**

Create an account and get your private key

Agree to the terms and conditions and submit

**Only if you are
Member of a
Tier1 project**

The screenshot displays a web form for creating a CÉCI account. At the top, there are three dropdown menus for selecting a university, faculty, and unit. The first dropdown shows 'Université de Namur' selected. The second dropdown shows 'Faculte de Medecine' selected. The third dropdown shows 'Unité d'analyse numérique' selected. Below these is section '4. Projects', which includes a text box with 'cecisys' and an 'Add project' button. A checkbox labeled 'I have read and agree to the terms and conditions.' is present. Section '5. Submit!' follows, with two options: 'Send' (a green button with a paper plane icon) and 'Save' (a blue button with a cloud icon). A blue arrow points from the red text on the left to the 'cecisys' text box.

Universite de Mons
Université de Namur
Université libre de Bruxelles

Faculte de Medecine
Patrimoines, transmissions, heritages

appliquees et complexe
Unité d'analyse numérique
Unité de statistiques

4. Projects

Projects allow access to supplementary resources, a. o. the Tier-1 cluster. Please make sure you have the authorization from the project owner before choosing one. You will need to know the acronym of the project.

cecisys Add project

☐ I have read and agree to the [terms and conditions](#).

5. Submit!

Once the form is completely filled-in, click the 'Send' button. A system administrator will review your request.

Send

If you want to save the current data and submit it later, click the 'Save' button.

Save

Create an account and get your private key

Wait ...

A sysadmin is reviewing your information



Create an account and get your private key

1. Sysadmin confirms the account.
2. Private and public key are generated
3. The private key is encrypted using the passphrase and **sent to you by email**



WARNING For security reasons

CÉCI does not keep a copy of your private key.

If you lose your key or passphrase or think it is compromised, you must **renew your CÉCI account** at

<https://login.ceci-hpc.be>

Create an account and get your private key



Exercise

Create your CÉCI account and get your private key

Create an account and get your private key

Save your identity file from the email and open a terminal

```
# Create ~/.ssh and move your private key into it
> mkdir -p ~/.ssh
> mv ~/Downloads/id_rsa.cecil ~/.ssh
# Set correct permissions
> chmod 600 ~/.ssh/id_rsa.cecil
# Generate your public key file
> ssh-keygen -yf ~/.ssh/id_rsa.cecil > ~/.ssh/id_rsa.cecil.pub
```

Create an account and get your private key

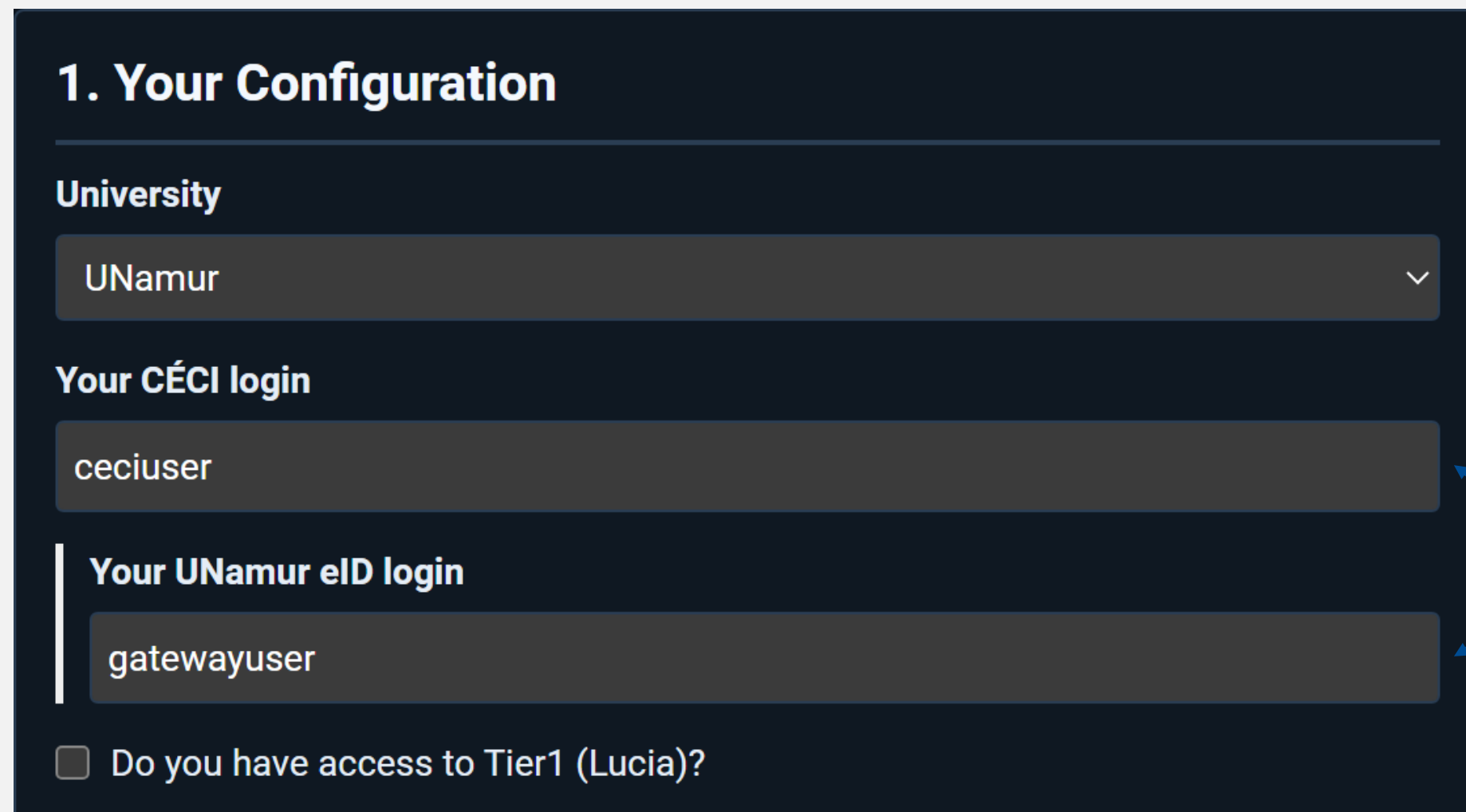
If you get “invalid format” or “error in libcrypto” error while generating the public key

```
# If you have the dos2unix command
> dos2unix ~/.ssh/id_rsa.cecici

# If you do not have dos2unix
> cp ~/.ssh/id_rsa.cecici ~/.ssh/id_rsa.cecici.bak
> tr -d '\r' < ~/.ssh/id_rsa.cecici.bak > ~/.ssh/id_rsa.cecici
```

Creating your configuration file

- Go to the CÉCI wizard <http://www.cec-hpc.be/sshconfig.html>
- Fill the form
- Depending on your university, the number of input fields will change.
- Tick the field "Tier 1" if you have access to Lucia.



The screenshot shows a dark-themed web form titled "1. Your Configuration". It contains three input fields: a dropdown menu for "University" with "UNamur" selected, a text field for "Your CÉCI login" containing "ceciuser", and a text field for "Your UNamur eID login" containing "gatewayuser". At the bottom, there is a checkbox labeled "Do you have access to Tier1 (Lucia)?" which is currently unchecked.

For UNamur members
your ceciuser = gatewayuser = your
UNamur Eid

Creating your configuration file

```
# University Gateway -----
Host gwceci
    Hostname gwceci.unamur.be
    User gatewayuser
    IdentityFile ~/.ssh/id_rsa.ceci

# CÉCI clusters -----
Host nic6 lyra lemaitre4 hercules nic5 dragon2 dragon3
    User ceciuser
    ForwardX11 yes
    IdentityFile ~/.ssh/id_rsa.ceci
    ProxyJump gwceci
    ServerAliveInterval 120
    ServerAliveCountMax 100

Host nic6
    Hostname nic6.uliege.be
Host lyra
    Hostname lyra.ulb.be
Host lemaitre4
    Hostname lemaitre4.cism.ucl.ac.be
Host hercules
    Hostname hercules.ptci.unamur.be
Host dragon2
    Hostname dragon2.umons.ac.be
Host dragon3
    Hostname dragon3.umons.ac.be
Host nic5
    Hostname nic5.uliege.be
```

Your gateway server ☐ GATEWAY

Your private Key

Common properties to all
frontends

☐ FRONTEND

Available frontend servers

☐ FRONTEND

Creating your configuration file

Copy the result

Edit (nano, vi, emacs ...) a **.ssh/config** file and **paste** the result

```
# Create and edit the config file
> nano ~/.ssh/config
# Set correct permissions
> chmod 600 ~/.ssh/config
```

Creating your configuration file



Exercise

Create your configuration file



Part 4

SSH connection

Connecting to a Frontend

Accept the public key of the CECI gateway
Stored in `~/.ssh/known_hosts` file

Connect to lemaitre4 frontend

```
> ssh lemaitre4  
The authenticity of host 'gwceci1.unamur.be (138.48.4.48)' can't be established.  
RSA key fingerprint is SHA256:GfUSNZEfZg28WRCaxJvDNSCCIhrX1IujNIky29ui7IY.  
This key is not known by any other names  
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

Verify fingerprint and accept

○ GATEWAY



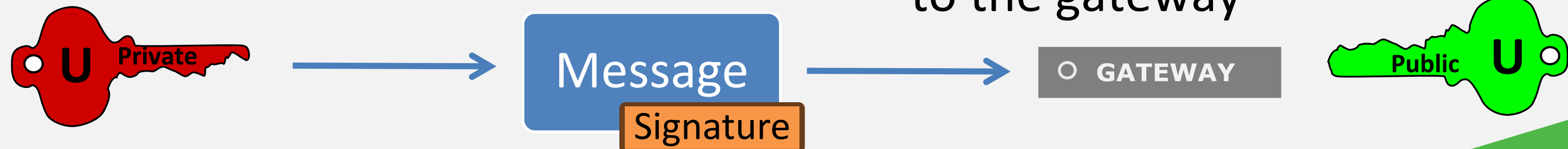
<https://support.cec-hpc.be/doc/QuickStart/ConnectingToTheClusters/FromAUnixComputer/#gateways>

Connecting to a Frontend

Connect to lemaitre4 frontend

```
> ssh lemaitre4
The authenticity of host 'gwceci.unamur.be (138.48.4.48)' can't be established.
RSA key fingerprint is SHA256:GfUSNZEfZg28WRCaxJvDNSCCIhrX1IujNIky29ui7IY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'gwceci.unamur.be' (RSA) to the list of known hosts.
Enter passphrase for key '/home/user/.ssh/id_rsa.ceci':
```

Decrypt your private key to sign a challenge message to authenticate to the gateway



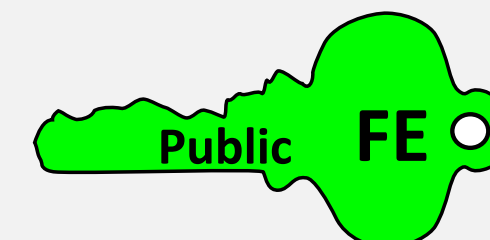
Connecting to a Frontend

Accept the public key of the frontend
Stored in `~/.ssh/known_hosts` file

Connect to lemaître4 frontend

```
> ssh lemaître4
The authenticity of host 'gwceci.unamur.be (138.48.4.48)' can't be established.
RSA key fingerprint is SHA256:GfUSNZEfZg28WRCaxJvDNSCCihX1IujNIky29ui7IY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'gwceci.unamur.be' (RSA) to the list of known hosts.
Enter passphrase for key '/home/user/.ssh/id_rsa.ceci':
The authenticity of host 'lemaître4.cism.ucl.ac.be (<no hostip for proxy command>)' can't be established.
ED25519 key fingerprint is SHA256:mWlgUkE+tBNbklXLgvrt7pL/30hn7uidqFfBUU0fSkQ.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

○ FRONTEND

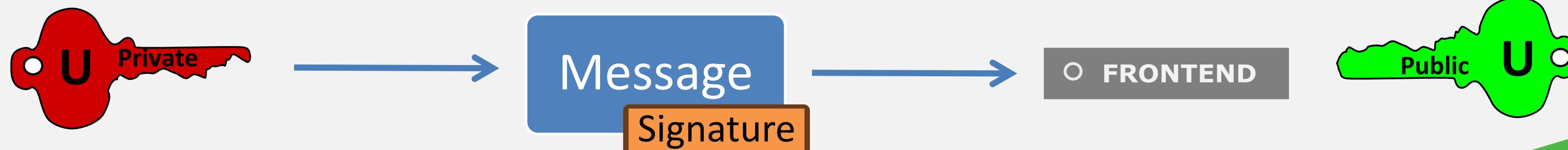


Connecting to a Frontend

Decrypt your private key to sign a challenge message to authenticate to the Frontend

Connect to lemaitre4 frontend

```
> ssh lemaitre4
The authenticity of host 'gwceci.unamur.be (138.48.4.48)' can't be established.
RSA key fingerprint is SHA256:GfUSNZEfZg28WRCax3vDNSCCIhrX1IujNIky29ui7IY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'gwceci.unamur.be' (RSA) to the list of known hosts.
Enter passphrase for key '/home/user/.ssh/id_rsa.cecil':
The authenticity of host 'lemaitre4.cism.ucl.ac.be (<no hostip for proxy command>)' can't be established.
ED25519 key fingerprint is SHA256:mWlgUkE+tBNbklXLgvrt7pL/30hn7uidqFfBUU0fSkQ.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'lemaitre4.cism.ucl.ac.be' (ED25519) to the list of known hosts.
Enter passphrase for key '/home/user/.ssh/id_rsa.cecil':
```



Connecting to a Frontend (X11 forwarding)

The **ForwardX11 yes** option in config file, allows you to run graphical programs on the frontend and display them on your local computer.

Try it: Connect to **lemaitre4** and run **xeyes** to test this feature.

```
[ceciuser@lm4-f001 ~]$ xeyes
```

macOS users need to install XQuartz (www.xquartz.org)



Connecting to a Frontend

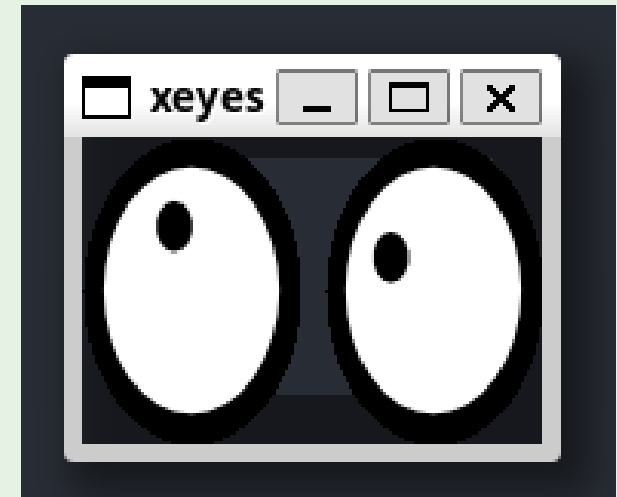


Exercise

Connect to **lemaitre4** frontend and execute **xeyes**
Use **ctrl-c** to stop xeyes
Use **exit** or **ctrl-d** to logout

Try connection to other clusters:

```
ssh lyra  
ssh hercules  
ssh nic6  
ssh dragon2  
ssh dragon3
```



SSH Agents, Passphrase managers

Use an SSH agent which will keep your decrypted key in memory, so you do not need to type your passphrase each time you issue the SSH command

```
# Check agent status
> ssh-add -l
# If you get this, your agent is not running
Could not open a connection to your authentication agent.
# If you get this, the agent is running but no key is loaded
The agent has no identities.
# If you get something like this, your private key is in memory
4096 SHA256:IrQnhTiZvW0FXKoZmdfoNmZt2dr3d86PDmxhd995nnA /home/user/.ssh/id_rsa.cecil (RSA)
```

SSH Agents, Passphrase managers

You can start the agent and add the private key

```
# Start the agent
> eval $(ssh-agent)
# Add the private key
> ssh-add ~/.ssh/id_rsa.cecil
Enter passphrase for /home/user/.ssh/id_rsa.cecil:
Identity added: /home/user/.ssh/id_rsa.cecil (/home/user/.ssh/id_rsa.cecil)
# Check agent status
> ssh-add -l
4096 SHA256:IrQnhTiZvW0FXKoZmdfoNmZt2dr3d86PDmxhd995nnA /home/user/.ssh/id_rsa.cecil (RSA)
# Try connection
> ssh lemaitre4
```

SSH Agents, Passphrase managers

You can have an ssh-agent started automatically at login by using password managing software such as

[Mac OS Keychain](#), [KDE KWallet](#), [Gnome Keyring](#) ([Seahorse](#)), etc.

Gnome Keyring loads all private keys in ~/.ssh folder **which have the corresponding public key**.

Mac OS users. Add those lines in the **config** file

```
Host *  
    AddKeysToAgent yes  
    UseKeychain yes
```

Troubleshooting

You can use -v, -vv or -vvv to troubleshoot a session

```
> ssh lemaitre4 -v
OpenSSH_8.9p1 Ubuntu-3ubuntu0.13, OpenSSL 3.0.2 15 Mar 2022
debug1: Reading configuration data /home/user/.ssh/config
debug1: /home/user/.ssh/config line 8: Applying options for lemaitre4
debug1: /home/user/.ssh/config line 18: Applying options for lemaitre4
...
debug1: Server host key: ssh-rsa SHA256:GfUS...i7IY
debug1: Host 'gwceci.unamur.be' is known and matches the RSA host key.
...
debug1: Offering public key: /home/user/.ssh/id_rsa.ceci RSA SHA256:IrQn...5nnA
debug1: Server accepts key: /home/user/.ssh/id_rsa.ceci RSA SHA256:IrQn...5nnA
Authenticated to gwceci.unamur.be ([138.48.4.48]:22) using "publickey".
...
debug1: Server host key: ssh-ed25519 SHA256:mWlg...fSkQ
debug1: Host 'lemaitre4.cism.ucl.ac.be' is known and matches the ED25519 host key.
...
debug1: Offering public key: /home/user/.ssh/id_rsa.ceci RSA SHA256:IrQn...5nnA
debug1: Server accepts key: /home/user/.ssh/id_rsa.ceci RSA SHA256:IrQn...5nnA
Authenticated to lemaitre4.cism.ucl.ac.be (via proxy) using "publickey".
```

1 Config file

your options are applied

2 Gateway

host key known, your key accepted

3 Frontend

same checks, through the gateway

Troubleshooting

Check for common errors in [CÉCI documentation](#)

Or copy-paste the output and create an issue

<https://support.cec-hpc.be/cecihelp/>



Part 5

SSH-based file transfer

SCP

You can copy files/directories back and forth between computers

```
# Create a temporary directory with dummy files on your computer
> mkdir -p cours_ssh/scp_test && touch cours_ssh/scp_test/file{1..4}.txt
# Run a command on the frontend (non-interactive session) to create a folder
> ssh lemaitre4 'mkdir -p cours_ssh'
# Copy the directory recursively into ~/cours_ssh/ on the lemaitre4 frontend
> scp -r cours_ssh/scp_test lemaitre4:cours_ssh/
# Check the content on the frontend
> ssh lemaitre4 'ls cours_ssh/scp_test/'
# Copy it back into a new scp_test2 folder (if it already exists, scp copies inside it)
> scp -r lemaitre4:cours_ssh/scp_test cours_ssh/scp_test2
# Check local copy
> ls cours_ssh/scp_test2
```



For copy between clusters. Use common [\\$CECIHOME](#) partition

rsync

rsync is widely used for backups and mirroring

```
# Create a folder and dummy files on the frontend
> ssh lemaitre4 'mkdir -p cours_ssh/rsync_test; touch cours_ssh/rsync_test/file{1..4}.txt'
# Check
> ssh lemaitre4 'ls cours_ssh/rsync_test/'
# Transfer it to your computer
> rsync -avz --progress lemaitre4:cours_ssh/rsync_test cours_ssh/
# Modify a file on the frontend and synchronize your local copy
> ssh lemaitre4 'echo "Adding hello1 word in $(hostname)" >> cours_ssh/rsync_test/file4.txt'
> rsync -avz --progress lemaitre4:cours_ssh/rsync_test cours_ssh/
# Check local copy
> cat cours_ssh/rsync_test/file4.txt
```

rsync

rsync is widely used for backups and mirroring

```
# Modify a file on your computer; -u keeps files that are newer locally
> echo 'Adding hello in client' > cours_ssh/rsync_test/file3.txt
> rsync -avzu --progress lemaitre4:cours_ssh/rsync_test cours_ssh/
# Check
> cat cours_ssh/rsync_test/file3.txt

# Delete a file on the frontend
> ssh lemaitre4 'rm cours_ssh/rsync_test/file1.txt'
# Check remote content (should fail: file deleted)
> ssh lemaitre4 'ls cours_ssh/rsync_test/file1.txt'
# Synchronize and delete local files removed on the frontend (--del)
> rsync -avzu --del --progress lemaitre4:cours_ssh/rsync_test cours_ssh/
# Check local content (should fail: file deleted)
> ls cours_ssh/rsync_test/file1.txt
```

SSHFS

Use SSHFS to mount a remote file system - accessible via SSH

Linux install

```
# Debian, Ubuntu, Mint  
> sudo apt-get install sshfs
```

```
# Fedora, CentOS, Rocky (CentOS/Rocky: enable EPEL first)  
> sudo yum install fuse-sshfs
```

Mac Os install

Install FUSE and SSHFS from <https://osxfuse.github.io/>

SSHFS

Example: Mount your [CECIHOME](#)

```
# Create a folder on your computer to mount your CÉCI home
> mkdir ceci_home
# Mount the remote CÉCI Home on your computer from Hercules
# (you can check with another frontend)
> cluster=hercules
> sshfs -o uid=$(id -u) -o gid=$(id -g) $cluster:$(ssh $cluster 'echo $CECIHOME')/ ceci_home
# Create a file in the mounted directory
> echo 'file content from my computer' > ceci_home/file_fuse.txt
# Check the file on the frontend and in the mounted folder
> ssh $cluster 'cat $CECIHOME/file_fuse.txt'
> ls ceci_home
# Unmount (on macOS: umount ceci_home)
> fusermount -u ceci_home
```

<https://www.unamur.be>

Juan Cabrera
Logisticien de Recherche

juan.cabrera@unamur.be

Rue de Bruxelles, 61 - 5000 Namur

