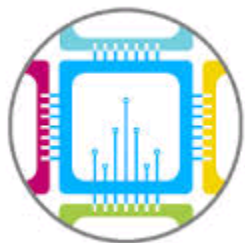


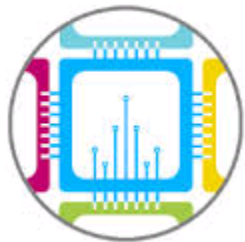
Генерация SSH ключей



Суперкомпьютерная
Академия

SSH

- SSH-ключ используется программой ssh (или другим ssh-клиентом) для авторизации на удаленном сервере
- Ключ состоит из двух частей: публичная часть и закрытая часть
- Не компрометируйте свою закрытую часть ключа!

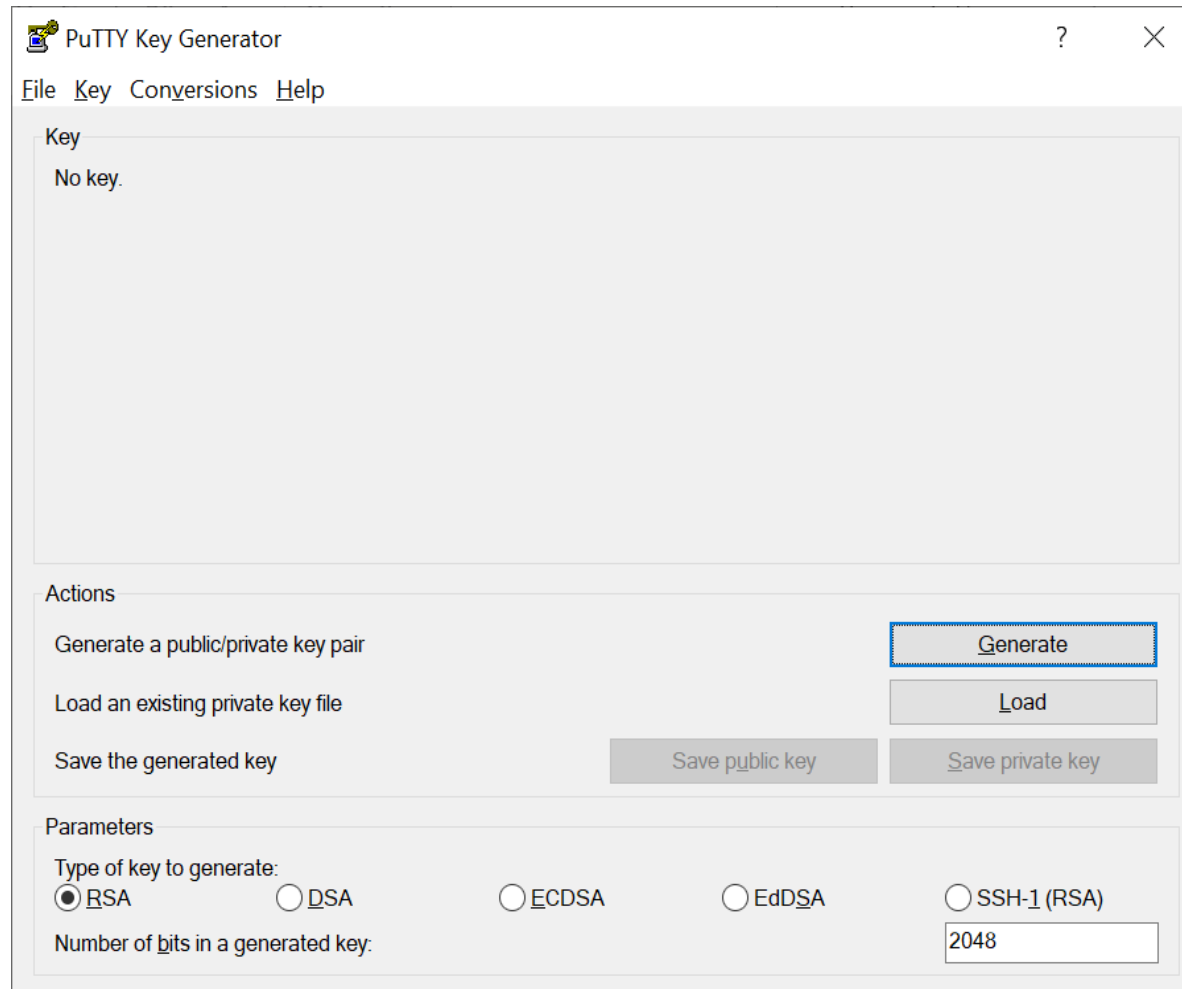


SSH. Windows

- ssh-клиент PuTTY
- PuTTYgen для создания ключа
- WinSCP для копирования файлов



SSH. Windows



The image shows a screenshot of the PuTTY Key Generator application window. The window title is "PuTTY Key Generator" and it has a menu bar with "File", "Key", "Conversions", and "Help". The main area is titled "Key" and contains the text "No key.". Below this is the "Actions" section with three rows of controls: "Generate a public/private key pair" with a "Generate" button, "Load an existing private key file" with a "Load" button, and "Save the generated key" with "Save public key" and "Save private key" buttons. The "Parameters" section includes "Type of key to generate:" with radio buttons for "RSA" (selected), "DSA", "ECDSA", "EdDSA", and "SSH-1 (RSA)", and "Number of bits in a generated key:" with a text box containing "2048".

PuTTY Key Generator

File Key Conversions Help

Key

No key.

Actions

Generate a public/private key pair

Load an existing private key file

Save the generated key

Parameters

Type of key to generate:

RSA DSA ECDSA EdDSA SSH-1 (RSA)

Number of bits in a generated key:



SSH. Windows

PuTTY Key Generator

File Key Conversions Help

Key

Please generate some randomness by moving the mouse over the blank area.

Actions

Generate a public/private key pair

Load an existing private key file

Save the generated key

Parameters

Type of key to generate:

RSA DSA ECDSA EdDSA SSH-1 (RSA)

Number of bits in a generated key:



SSH. Windows

PuTTY Key Generator

File Key Conversions Help

Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa  
AAAAB3NzaC1yc2EAAAADAQABAAQCFaTe5IRSpUSwbbUH2RK90CHcl9FRqQwIWDHQnf3bGqm3osY4  
709yiZ7pTgQ5dirGPMFaVforTuzYNMO0wyXn0uHWI7fluvB3JL6XFIJzLT3XJwjeg1K2AzOf3SEV9p  
+C/ZY6zcjic5DyY6CrQErO7PFIBSGUY/hiYojXPUS/1/hErRBbc1nC4bmZ/h3A87VOaHZB9BH5DBj4nfxu  
+w8A7pN1OCULhreMRTIOqV4SMwZqMTg8DmTE9vJTInICLU+dg8GBgMgmNKm3h4b
```

Key fingerprint: ssh-rsa 2048 SHA256:D5DfAYy7jxGVuk+FD+ie0OemSzFEmMv3g59n66SDBJs

Key comment: rsa-key-20211011

Key passphrase:

Confirm:

Actions

Generate a public/private key pair

Load an existing private key file

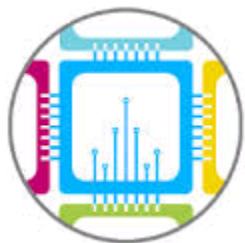
Save the generated key

Parameters

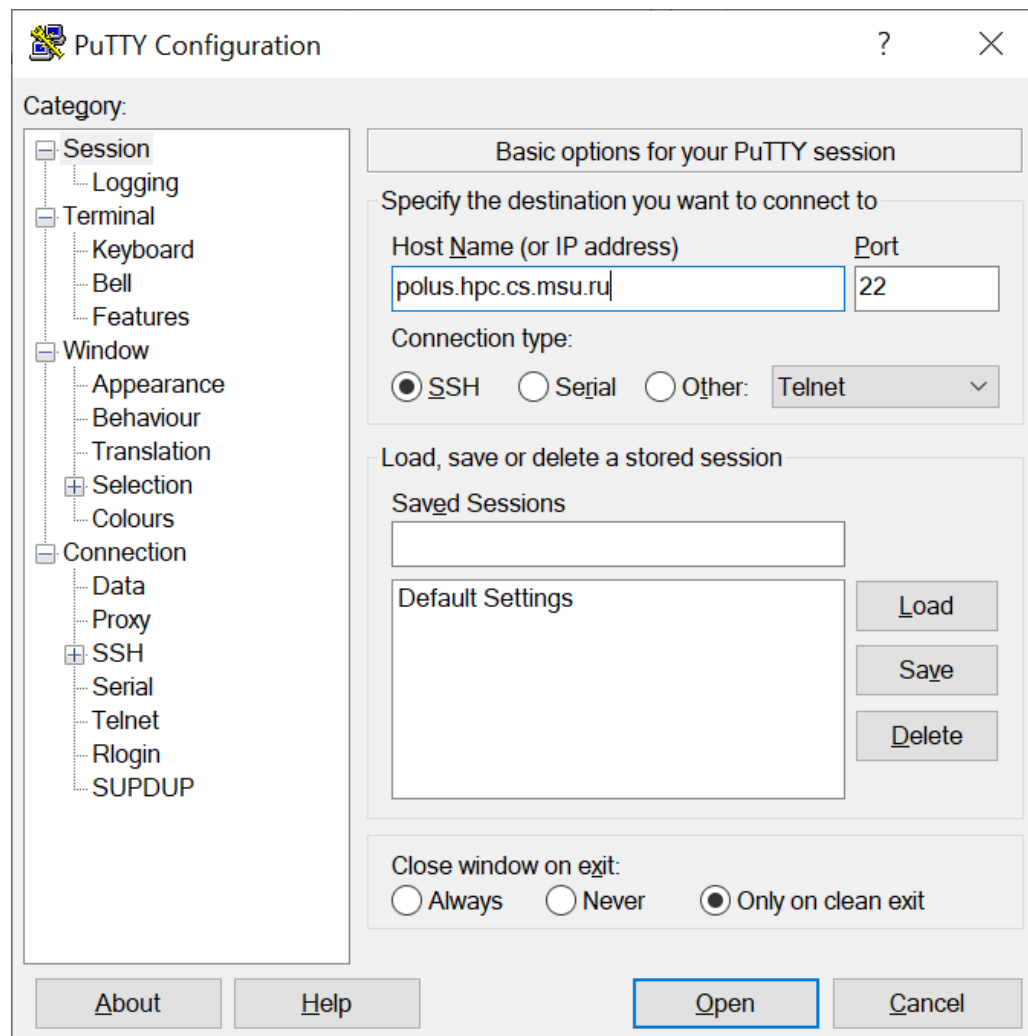
Type of key to generate:

RSA DSA ECDSA EdDSA SSH-1 (RSA)

Number of bits in a generated key: 2048



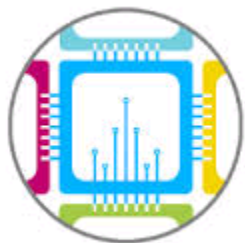
SSH. Windows



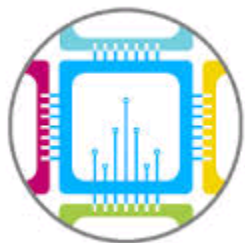
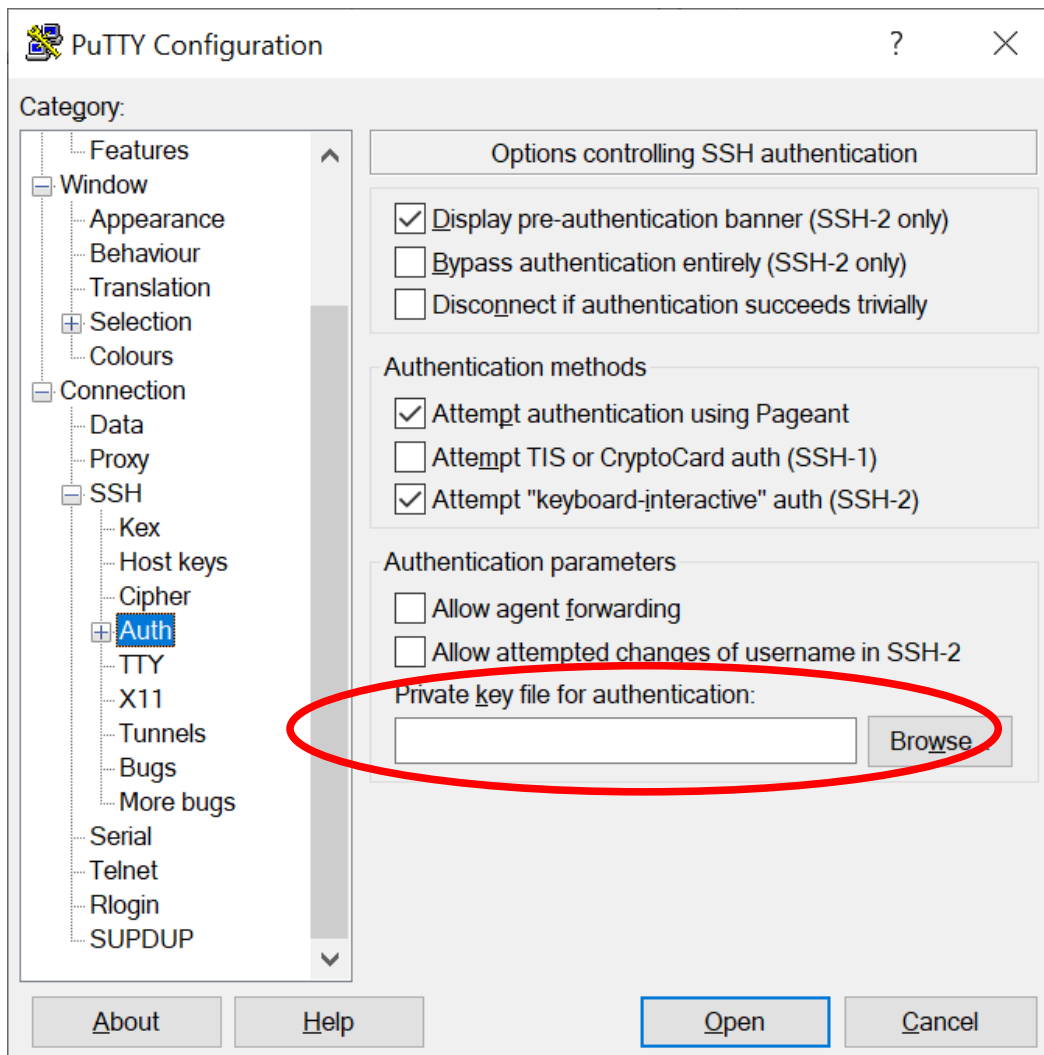
The image shows the PuTTY Configuration dialog box. The title bar reads "PuTTY Configuration" with a help icon and a close button. On the left is a tree view under "Category:" with the following items: Session (expanded), Logging, Terminal (expanded), Keyboard, Bell, Features, Window (expanded), Appearance, Behaviour, Translation, Selection (expanded), Colours, Connection (expanded), Data, Proxy, SSH (expanded), Serial, Telnet, Rlogin, and SUPDUP. The main area is titled "Basic options for your PuTTY session" and contains the following fields and controls:

- Section: "Specify the destination you want to connect to"
- Host Name (or IP address):
- Port:
- Section: "Connection type:"
- Radio buttons: SSH, Serial, Other:
- Dropdown menu: Telnet
- Section: "Load, save or delete a stored session"
- Text box: Saved Sessions
- Text box: Default Settings
- Buttons: Load, Save, Delete
- Section: "Close window on exit:"
- Radio buttons: Always, Never, Only on clean exit

At the bottom of the dialog are buttons for "About", "Help", "Open", and "Cancel".



SSH. Windows



SSH. Linux

- ssh-клиент уже есть в системе
- Если нет, то: `sudo apt-get install openssh-client`



SSH. Linux

- Перед созданием ключа убедитесь, что он еще не создан: `ls -l ~/.ssh`
- Если в выводе файлы `id_rsa/id_dsa`, то нужный ключ уже есть, создавать не требуется



SSH. Linux

- `ssh-keygen -t rsa -b 4096 -f ~/.ssh/id_rsa_hpc`
- закрытый ssh-ключ (identification) будет сохранен в `~/.ssh/id_rsa_hpc`
- открытый ssh-ключ (public key) будет сохранен в `~/.ssh/id_rsa_hpc.pub`



SSH. Linux

- Получение fingerprint:
`ssh-keygen -l -f ~/.ssh/id_rsa_hpc.pub`
- Переименовать ключ `edu-acad2023-Nxx.pub`
- Адрес для ключей: `academy-hpc@yandex.ru`
- Еще более подробно
<https://wiki.cs.msu.ru/Main/SSHKeysManual>

