1/5

# Usando chave do ssh

# O que é chave do ssh e por quê usá-la?

A chave de ssh é uma credencial que permite o detentor da chave acessar um servidor ssh. Ela consiste na verdade em um par de chaves: uma privada e outra pública. A chave privada deve ser guardada com segurança e, idealmente, não compartilhada. A pública deve ser colocada no servidor ssh de destino para a autenticação.

A chave ssh é uma alternativa à senha. Ela é mais segura pois não necessita transferir a senha ao servidor, possui tamanho maior e mais complexo do que qualquer senha que o usuário possa ter e permite acesso mais fácil ao servidor, sem ter precisar lembrar de senhas.

# Como criar uma chave ssh e transferir para o servidor

# **Host Linux**

## Criar um par de chaves

Para criar um par de chaves com as opções padrões, basta rodar o comando ssh-keygen e responder as perguntas interativamente. Supondo *username* como o seu nome de usuário **local** e *hostname* como o host name de sua máquina:

```
> ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/<username>/.ssh/id rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/<username>/.ssh/id rsa
Your public key has been saved in /home/<username>/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:rwnGdXmwaCQvlAfoNsbfQz8jmKkmgwlrzHzH4rPkcBI @<hostname>
The key's randomart image is:
+---[RSA 3072]---+
      . .
        0
     •
    0 + 0.
     *. =.. +
 E o o.*S.+ .
      .=++0+.
|=* 0..+ 0.0
|+=0+o+ . o
|. oB=
         0
+----[SHA256]----+
```

Pode-se alterar o nome e o caminho das chaves e, opcionalmente, adicionar uma senha associada à

chave. A senha será perguntada ao usuário tentar logar no servidor com a chave pública, a fim de aumentar a segurança. Recomenda-se utilizar a pasta e os nomes padrões para facilitar o próximo passo.

#### Adicionar a chave pública ao servidor

No exemplo será usado o servidor sites.ime.usp.br como o servidor ssh. Além disso, *server username* é o nome do usuário no **servidor**.

> ssh-copy-id -i <pub\_key\_file> -p <port\_num>
<server\_username>@sites.ime.usp.br
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to
filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are
prompted now it is to install the new keys
<server\_username>@sites.ime.usp.br's password:

```
Number of key(s) added: 1
```

```
Now try logging into the machine, with: "ssh
'<server_username>@sites.ime.usp.br'"
and check to make sure that only the key(s) you wanted were added.
```

A flag -p <port\_num> é opcional e especifica a porta do servidor caso não seja a padrão 22. A -i <pub\_key\_file> especifica o caminho da chave pública (nome colocado ao criar com o ssh-keygen com o final .pub), sendo opcional caso tenha usado o caminho padrão na criação das chaves.

O comando pergunta interativamente a senha do servidor ssh do seu usuário para copiar a chave.

#### Acessando o servidor

Com as chaves criadas e a pública copiada, o usuário pode acessar o servidor com o comando ssh i <pub\_key\_file> -p <port\_num> '<server\_username>@sites.ime.usp.br'. Assim como no comando anterior, as flags -i <pub\_key\_file> e -p <port\_num> são opcionais. A senha da chave, caso tenha sido criada, será perguntada interativamente.

# **Host Windows**

# Instale o PuTTY

Acesse o link https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html e baixe o instalador do \*PuTTY\*. Execute o instalador.

#### Logue no sites.ime.usp.br

Abra o programa **PuTTY** e insira sites.ime.usp.br no campo Host Name e clique em Open. Logue e deixe a janela aberta para os próximos passos.

	PuTTY Configuration	×
Category: Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Colours Colours Colours Source Serial Telnet Riogin SUPDUP	Basic options for your PuTTY ses Specify the destination you want to conner Host Name (or IP address) [sites.ime.usp.br] Connection type: © SSH O Serial O Other: Telnet Load, save or delete a stored session Saved Sessions Default Settings Close window on egit: C Always O Never O Only on d	ect to Port 22 Load Saye Delete ean exit
About Help	Qpen	⊊ancel

# Criando as chaves

Execute o programa **PuTTYgen**, crie as chaves clicando no botão Generate e copie a chave pública.

PuTTY Key Generator	×
Elle Key Conversions Help	
Key	
Public key for pasting into Open55H authorized_keys file: kety-rea AAAA83NaaC1wt2EAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	-
+ /1C02PmVcuDLriO//AntkRDietpP4ZEEL90/gNq15YkhT jGkP jqU/	
uPts6x9ztSTCCoKPy1ybguBhc+qY68h1nBNKijYyZjw87RXtxryKen4tjq55sgMIP5fWFOCGWnE5X5PyYee	UJB
+h22jblp+aLAET6SIVsmYPCcTqH9ZWpdsvbHJmNH+Q1MM4DrDfyO+mPTyFVF5an1kCChyKT3rWUVo	
Key fingerprint: ssh-rsa 2048 SHA256:46QZ/8K0XJmol/L+M0rqvYyaBIJU65vDIpA85/SIhXc	
Key comment: rsa-key-20230309	
Key passphrase:	
Cgnfirm	
Actions	
Generate a public/private key pair General	te
Load an avieting petrate law file	
Load an executive revine	
Save the generated key Save public key Save privat	e key
Parameters	
Type of key to generate:	
ESA CESA CECUSA CECUSA	(SA)
number or girs in a generated way: 2048	

### Adicionar a chave pública no servidor

No servidor logado no **PuTTY** edite, com seu editor de texto favorito, o arquivo \${HOME}/.ssh/authorized\_keys para acrescentar a chave copiada no passo anterior e feche a sessão.

#### Salvar a chave privada

Clique no botão Save private key no PuTTYgen e salve em um lugar apropriado.

#### Adicionar chave privada ao PuTTY

No **PuTTY**, vá em Connection > SSH > Auth > Credentials e adicione o arquivo salvo no passo anterior em Private key file for authentication.

PuTTY Configuration ×		
Category:		
Keyboard 🔺	Credentials to authenticate with	
Bell	Public-key authentication	
Features	Private key file for authentication:	
⊡ Window	Culture gray File (Dr. Trylether, Inc. und	
Appearance	C:(Program Files(Pull 11(sices_ime_usp.) Browse]	
Behaviour	Certificate to use with the private key:	
Translation	Browse	
E Selection	·	
Colours	Plugin to provide authentication responses	
E- Connection	Plugin command to run	
Provv		
E-SSH		
Kex		
- Host keys		
Cipher		
E Auth		
Credentia		
GSSAPI		
TTY		
About Help	Qpen	

Com isso você consiguirá logar no sites.ime.usp.br usando a chave do ssh através do programa **PuTTY**.



Wiki da Rede IME - https://wiki.ime.usp.br/