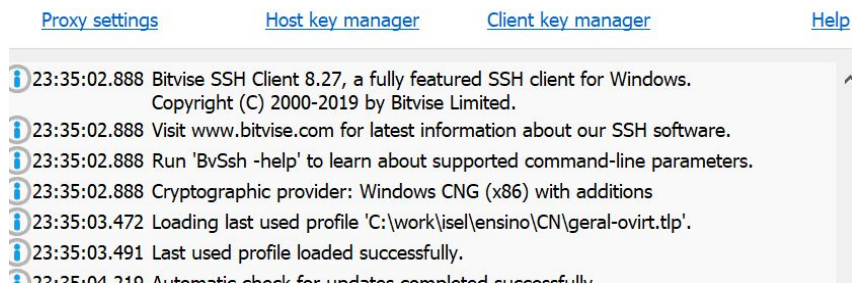


## Laboratório 3 - Preparação

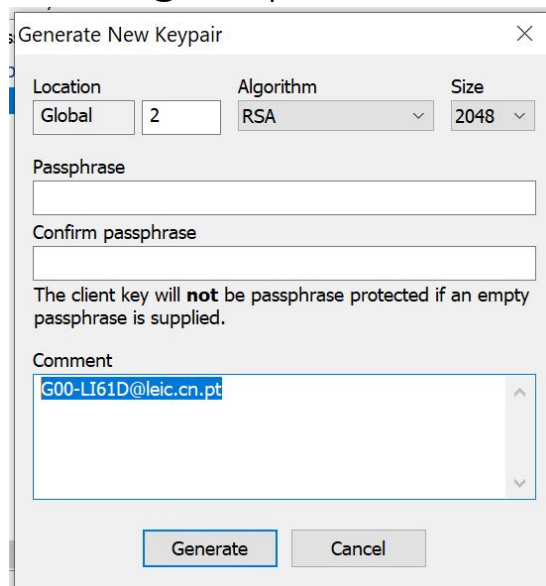
1. As máquinas virtuais criadas no GCP são acedidas via SSH com autenticação de chave pública. O guião seguinte mostra como gerar um par de chaves pública/privada com o cliente SSH Bitvise em Windows:

*Para outros sistemas operativos, e outros clientes, sugerimos a consulta das instruções em <https://www.ssh.com/ssh/keygen/>, onde são usadas ferramentas de linha de comando para produzir o mesmo resultado.*

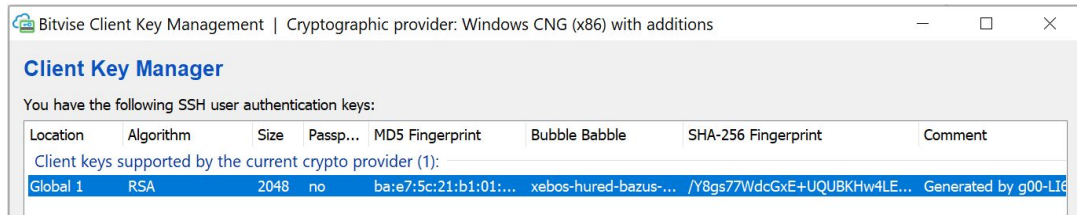
- a. No cliente Bitvise aceda a “Client Key Manager”



- b. Na zona inferior da janela, escolha “Generate New”
- c. Escolha uma password para proteger a chave privada, ou deixe em branco. **Na caixa de comentário** (“Comment”) indique um identificador com o formato <nome>@cn.isel.pt. Sugere-se o nome do grupo como no projeto GCP, ex: G00-LI61D@cn.isel.pt.



- d. Selecione “Generate” para gerar o par de chaves e acrescentar à lista de chaves disponíveis no cliente Bitvise:



- e. Exporte a chave pública escolhendo a opção “Export” da mesma janela. Indique o formato “OpenSSH” e exporte a chave pública para um ficheiro e diretoria à sua escolha.
- f. Visualize a chave pública exportada com um editor de texto (ex: code, notepad, ...).
2. Usando a conta GCP do grupo, crie 1 máquina virtual do tipo ‘f1.micro’, selecionando a opção correspondente no menu “Machine type”:
- a. Ative HTTP e HTTPS na firewall.
- b. Click em “Management, security, disks, networking, sole tenancy” e depois no tab “Security”. Copie a chave pública SSH gerada no ponto 1 para o formulário disponível. Note que o formato imposto pelo formulário é: <protocol> <key-blob> <username@example.com>, o qual corresponde ao formato da chave gerada no ponto 1.c no *edit box Comment*.  
Atenção ao fazer *copy/paste* a partir do ficheiro, onde guardou a chave no ponto 1.e, verificando que a última linha não tem um <Enter>.

**Firewall** ?  
Add tags and firewall rules to allow specific network traffic from the Internet.

☐ Allow HTTP traffic  
☐ Allow HTTPS traffic

Management **Security** Disks Networking Sole Tenancy

**Shielded VM** ?  
Select a shielded image to use shielded VM features.  
Turn on all settings for the most secure configuration.

☐ Turn on Secure Boot ?  
☐ Turn on vTPM ?  
☐ Turn on Integrity Monitoring ?

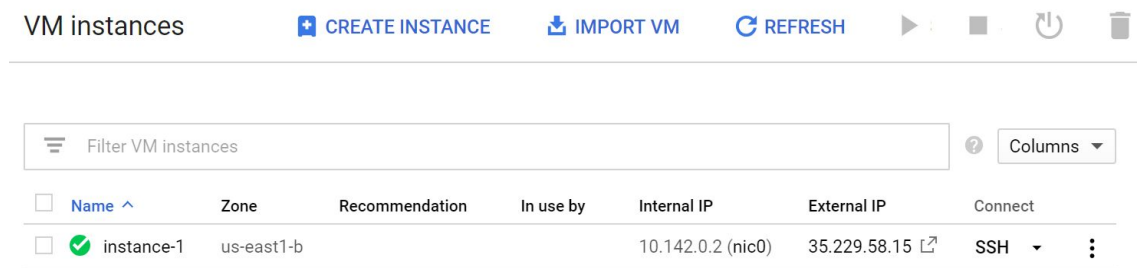
**SSH Keys**  
These keys allow access only to this instance, unlike [project-wide SSH keys](#) [Learn more](#)

☐ Block project-wide SSH keys  
When ticked, project-wide SSH keys cannot access this instance. [Learn more](#).

G00-LI61D

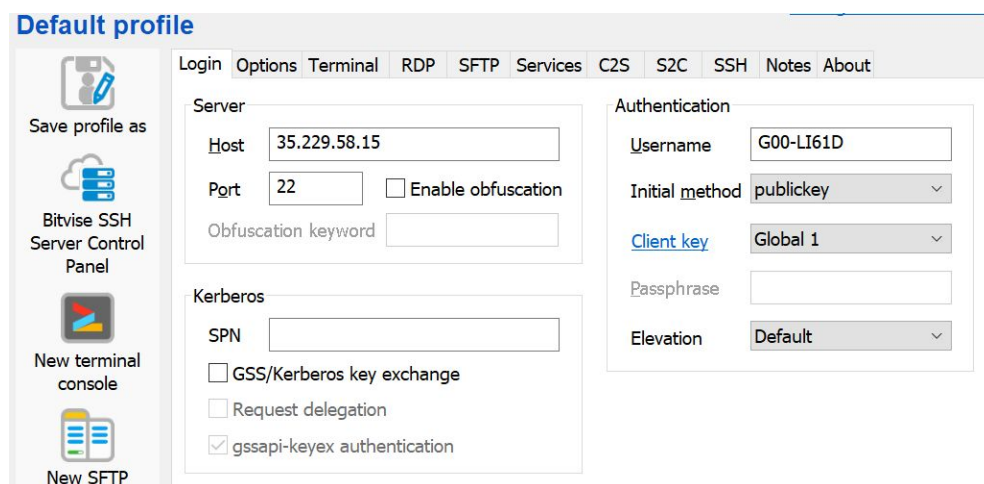
```
MBH3s8Taz4J41zg747AXbdRuqU6UNVFZyEtGcZ6+A  
jZCp6U1ExU+1cpxLKa7bv1jrDVm/SRmKcH30a/2BQ  
KZfPRh2yeWM54TYitov0gTg5NYXyTc6oE/RGi0wq6  
yvwWJ6GgL+4BddnWZ0kiW2KcPvW+qRheAXj//3zR9  
jbbJpus5khicxYR06I318ErubyX8HwZkEMt0/d8V+  
rgjcM1Xcv5f3EyWtCu1pTc8PWeTGDL79jgy4NvAci  
cSofJ4QnJvB G00-LI61D
```

- c. Crie a VM e verifique na consola Web do GCP que a máquina foi iniciada e tem um IP externo:



<input type="checkbox"/>	Name ^	Zone	Recommendation	In use by	Internal IP	External IP	Connect
<input type="checkbox"/>	instance-1	us-east1-b			10.142.0.2 (nic0)	35.229.58.15	SSH

- d. Aceda à VM através do cliente SSH. O utilizador é o indicado no ponto 1.c), ex: G00-LI61D, o método inicial é “public key” e a “Client key” tem de indicar a entrada criada anteriormente no ponto 1.d).



- e. Após login, verifique o correto acesso à VM. Não se esqueça de desligar a VM quando não a estiver a usar, usando o botão “Stop” na consola Web do GCP.



```
G00-LI61D@instance-2:~$ cat .ssh/authorized_keys
# Added by Google
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDcuct4o7LCPfEsFWg3puSmHojqBeYk00YtIyJBojfcF5mFIYVe
RdOHsoJmJWz1Uu1AhQImZor21Y6j2YJmmqOMBH3s8Taz4J41zg747AXbdRuqU6UNVFZyEtGcZ6+AjZCP6U1EXU+1
cpxLKa7bv1jrDVm/SRmKch30a/2BQKZfPRh2yeWM54TYitov0gTg5NYXyTc6oE/RG10wq6ywwWJ6GgG+4BddnWZ0
kiW2KCpvW+qRheAXj//3zR9jbBJpus5khicxYR06I318ErubyX8HwZkEMt0/d8V+rgjcM1Xcv5f3EyWtCu1pTc8P
WeTGD79jgy4NvAcicSofJ4QnJvB G00-LI61D
G00-LI61D@instance-2:~$
```

3. A máquina virtual agora instanciada tem apenas a base do sistema operativo. Ferramentas como o JDK, git, ou outras, terão de ser instaladas usando os comandos e repositórios associados ao sistema operativo escolhido. Esta é uma das diferenças entre o modelo de serviço IaaS e PaaS.
  - a. A título de exemplo indica-se o comando para instalar o JDK 8 num sistema operativo Debian/Ubuntu:

```
sudo apt install openjdk-8-jdk
```