CLAVE RSA EN DRAGO CON PUTTY

Dependiendo de la plataforma utilizada (Windows, Mac o Linux) para conectarse al HPC Drago, los pasos generales a seguir para la generación y uso de una clave RSA están publicados en el Portal Documentación AIC (SGAI)

https://docaic.rstools.csic.es/es/home

Este manual explica los pasos específicos a seguir en este proceso para realizarlo mediante el uso del software PuTTY/PuTTYgen que el usuario debe tener instalado en el PC.

1. <u>GENERACION DE LAS CLAVES</u>

El primer paso consiste en generar las claves publica (la que se copia en Drago) y privada (la que el usuario utiliza para identificarse) mediante PuTTYgen. Para ello, abrimos el software y presionamos el botón de "Generate"

😴 PuTTY Key Generator			? ×
File Key Conversions Help			
Key No key.			
Actions			
Generate a public/private key pair			Generate
Load an existing private key file			Load
Save the generated key		Save public key	Save private key
Parameters			
Type of key to generate: RSA ODSA	O ECDSA	CEdDSA	🔿 SSH-1 (RSA)
Number of bits in a generated key:			2048

A continuación, se abrirá una ventana en la que debemos mover el ratón de forma aleatoria para que se vayan generando las claves.

😴 PuTTY Key Generator			? ×
File Key Conversions Help			
Key			
Please generate some randomness by mo	ving the mouse ov	er the blank area.	
1000000-0-0			
Actions			
Generate a public/private key pair			Generate
Load an existing private key file			Load
Save the generated key		Save public key	Save private key
Parameters			
Type of key to generate:	○ FCDSA		SSH-1 (RSA)
Number of bits in a generated key:	CEBBOA	Cabort	2048

Una vez generadas las claves, que aparecen en el apartado "Key" de la ventana, es necesario exportar ambas claves (pública y privada) a sendos ficheros.

Para guardar la clave publica, pulsamos sobre el botón "Save public key" y guardamos la clave con el nombre de fichero que nos permita reconocerlo.

2	PuTTY	Key Gener	ator						?	×
File	Key	Conversi	ons	Help						
Ke Pu s: A n +	ey ublic key sh-rsa (AAAB3) HZddyF aZiuiLF1	y for pasting NzaC1yc2E R/AtTBQ50 hdE003zhk	into AAA/ a8kr\$ BJgtf	OpenSSH aut ADAQABAAAB Mod0g5UgTMx R4B2cfmec1Jt	horized_keys file: BAQCKnJ1CH7S0V MukAnfPGPa Ggox6FERrCf6olwe	VYZE ebn2	3mtyZQvBHAGMLzP401L ATXywct9Zepah3VXUfBg	bFMEcQFOsStd 1m98+JU2fWdI6	BiAp Um 5xuuuG	
Ka Ka Ka	ey finger ey comn ey passp onfirm pa	nprint: nent: ohrase: assphrase:	ssh+ rsa+	rsa 2048 SHA xey-20250306	256:/E0s6RLzE+/;	zZP5	/nv4e77v+YaMpEZiApeC	ChYLmD/ag		
Ac Ge Lo Sa	ctions enerate pad an e ave the	a public/pri existing priva generated k	vate l ate ka key	key pair :y file			Save public key	Genera Load Save priva	te te key	
Pa Ty N	arameter ype of k RSA umber o	rs ey to gener f bits in a ge	ate: C) DSA ted key:	⊖ ECDSA		⊖ EdDSA	○ SSH-1 2048	(RSA)	

😴 Save public key as:					×
\leftrightarrow \rightarrow \checkmark \uparrow \square > Escr	itorio > clave		~ 0	Buscar en clave	م
Organizar 👻 Nueva carpeta					≣ • 😗
A Inicio	mbre	Fecha de modificación	Тіро	Tamaño	
🛃 Galería	Ning	ún elemento coincide con e	el criterio de búsqueda.		
> 🔊 Nextcloud					
> 📩 OneDrive					
🛄 Escritorio 🏾 🖈					
🚽 Downloads 🖈					
📔 Documentos 🖈					
🔀 Imágenes 🖈					
Nombre: clave_publica					~
Tipo: All Files (*.*)					~
∧ Ocultar carpetas				Guardar	Cancelar

Para guardar la clave privada, pulsamos sobre el botón "Save private key"

😴 PuTTY Key Generator	?	\times
File Key Conversions Help		
Key		
Public key for pasting into OpenSSH authorized_keys file:		
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCKnJ1CH7S0WYZBmtyZQvBHAGMLzP401LbFMEcQFOsSi nHZddyR/AtTBQ5Oa8kr9bd0g5UgTMxMukAnfPGPa +aZiuiLFndEO03zhkBJgtR4B2cfmec1Jt6gox6FERrCf6olwebn2ATXywct9Zepah3VXUfBgrm98+JU2fWd L5pHJzmalbB	:dBiApUm 165xuuuG	I
Key fingerprint: ssh-rsa 2048 SHA256:/E0s6RLzE+/zZP5/nv4e77v+YaMpEZiApeChYLmD/ag		
Key comment: rsa-key-20250306		
Key passphrase:		
Confirm passphrase:		
Actions		
Generate a public/private key pair Gene	rate	
Load an existing private key file	ad	
Save the generated key Save public key Save privately Save private	vate key	
Parameters		
Type of key to generate: ● RSA ○ DSA ○ ECDSA ○ EdDSA ○ SSH-	1 (RSA)	
Number of bits in a generated key: 2048		

En este caso, dado que la clave privada únicamente debe tenerla y usarla el usuario que se identifica, se puede proteger mediante una contraseña rellenando el apartado de "Key passphrase" y su réplica "Confirm passphrase".

Hay que tener en cuenta que esta contraseña será necesario introducirla cada vez que se utilice la clave para identificarse por lo que, si estamos en un PC que solo utilizamos nosotros, se puede dejar en blanco. En caso contrario, es recomendable rellenarlo para evitar que otros usuarios se identifiquen en Drago con nuestro

usuario. Si la "Key passphrase" se deja vacía, el programa nos preguntara si queremos seguir sin esa protección.



A continuación, guardamos la clave con el nombre de fichero que nos permita reconocerlo.

😴 Save private key as:		×
\leftarrow \rightarrow \checkmark \uparrow \bigcirc Escritorio \Rightarrow clave	✓ C Buscar en clave	Q
Organizar 👻 Nueva carpeta		- ()
☆ Inicio	Fecha de modificación Tipo Tamaño	
🔁 Galería	Ningún elemento coincide con el criterio de búsqueda.	
> 🔊 Nextcloud		
> 🛅 OneDrive		
📒 Escritorio 📌		
🛓 Downloads 🖈		
Documentos *		
Nombre: privada		~
Tipo: PuTTY Private Key Files (*.ppk)		~
∧ Ocultar carpetas	Guardar Ca	ncelar

2. CONFIGURACION DE LA CLAVE EN DRAGO

Una vez disponemos de las claves, es necesario copiar la clave publica en nuestro usuario de Drago. Para ello:

 En nuestro PC, abrimos el fichero con la clave publica que hemos generado con el Notepad y copiamos únicamente la clave (en la imagen, sería lo que está dentro del recuadro rojo)

Archivo	Editar	Ver
BEG	TN SSH2	PUBLIC KEY
Comment:	"rsa-ke	
AAAAB3Nz	aC1yc2EA	VAAADAQABAAABAQCUXeDYyHne+TZI8uWCau9BLfFXC1mWWyuJ
ht+Xqliw	1iK2hLd9	<pre>VXGvLA3Q9a/0xuOspvrLZ78hDR1rBweP20fgBE1GitzKD7FC</pre>
IM1rbfv2	wCPg2y4t	:VKpgUxvpNbtMkWTLqqsYFAVnq+k21RBwcKbJBDIVWGFw5J1k
+IKvr0TI	DamlPWdb	<pre>>zoP+8UTmaazPk/oCqK6sfns/9NTBUA57xSY1ACqH14cSvW4v</pre>
iAFGzPze	A5ti557E	WKzeN2mTK0WmWlqdCB3IoMLyv/Opiv+gu99G6BdneTBqQjK1
Pfr0Kj2K	CQQxsuDS	rE5xMH6f9SE8miBwjH2t7mQ1YFA07h5moPZV
END	SSH2 PU	IRTIC KEA

- Iniciamos sesión en Drago
- Nos aseguramos de estar en nuestra carpeta home con el comando



• Ejecutamos el siguiente comando



Esto abrirá el fichero "authorized_keys" si existe. Si no existe, se creará al editarlo y guardarlo.

• En este editor, comenzamos escribiendo una nueva línea con "ssh-rsa" y a continuación, pegamos la clave que previamente hemos copiado

GNU nano 2.	9.8	p	rueba		Modified
ssh-rsa AAAAB	3NzaClyc2EAAAAI	DAQABAAABAQCUX	eDYyHne+TZI8u	WCau9BLfFXC1m	WWyuJ
ht+XqliwliK2h	Ld9VXGvLA3Q9a/(xuOspvrLZ78hD	R1rBweP2OfgBE	lGitzKD7FC	
IM1rbfv2wCPg2	y4tVKpgUxvpNbt1	1kWTLqqsYFAVnq	+k21RBwcKbJBD	IVWGFw5J1k	
+1Kvr0T1Dam1F	WdbzoP+80Tmaaz	Pk/oCqK6sins/9	NTBUA57xSYIAC	qH14cSvW4v	
1AFGZPZEA5t15	57EWKZENZMIKUWI	nwiqacB3ioMLyv PriBuil2+7mOlV	/Opiv+gu99G6B	anersqQJKI	
FIIONJZACQQXS	ubsteskin6195E	SMIIDWJH2C/MQII	FA07H5III0P2V		
^G Get Help	^0 Write Out ^1	Where Is ^K	Cut Text ^J	Justify ^C	Cur Pos
^X Exit	^R Read File ^\	Replace ^U	Uncut Text [^] T	To Spell ^	Go To Line

• Eliminamos los saltos de línea para que todo esté en una única línea GNU nano 2.9.8

sh-rsa AAAAB3NzaClyc2EAAAADAQABAAABAQCUXeDYyHne+TZI8uWCau9BLfFXC1mWWyuJht+XqliwliK2hLd9VXGvLA3Q9a/0xuOspvrL

- Guardamos el fichero y salimos del editor.
- Modificamos los permisos del fichero para que solo pueda acceder el propietario mediante el comando



3. CONFIGURACION DE LA SESION EN PUTTY

Una vez disponemos de la clave publica en Drago, solo es necesario configurar nuestra sesión en PuTTY para conectarnos. Para ello, abrimos el PuTTY y rellenamos los datos de la sesión.

🕵 PuTTY Configuration					?	\times
Category:						
E. Session		Basic option	s for your Pu	TTY ses	sion	
i Logging ⊡ Terminal	Specify th	e destination	n you want to	connec	t to	
Keyboard Bell	drago.csi	ie (or iP add ic.es	ress)		22	
Features	Connectio	on type:				
Window Appearance	O SSH	⊖ Serial	Other:	Telnet		~
Behaviour Translation Translation Selection Colours Connection Data Proxy SSH Serial Telnet Rlogin	Load, sav	e or delete a	i stored sessi	on	Loa Sav Dele	d e te
SUPDUP	Close win	dow on exit: s ONev	er 🔾 On	ly on cle	ean exit	
About Help			Open		Cano	el

Configuramos la clave privada, seleccionando "Connection / SSH / Auth / Credentials" en la ventana de "Category"

RuTTY Configuration		?	\times
Putty Configuration Category: Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Data Proxy SSH Kex Host keys Cipher Auth Credentials GSSAPI TTY X11	Credentials to authenticate with Public-key authentication Private key file for authentication: C:\Users\Dell\Desktop\clave\clave_pr Certificate to use with the private key (option Plugin to provide authentication responses Plugin command to run	? Browse.	
About Help	Open	Cancel	

Y pulsamos sobre le boto "Browse" en "Private key file for authenticate". Esto nos permite seleccionar el fichero donde se encuentra almacenada la clave privada.

Una vez seleccionado, volvemos a la pestaña de "Session" y guardamos la configuración de la sesión con un nombre.

🕵 PuTTY Configuration		? ×
Category:		
- Session	Basic options for your PuTTY	session
Logging	Specify the destination you want to com	nect to
]. Terminal	Host Name (or IP address)	Port
- Rell	drago.csic.es	22
Features	Connection type:	
Window	SSH Serial Other: Tel	net 🗸
Behaviour	Load, save or delete a stored session	
Translation	Saved Sessions	
	usuarioDrago	
Data		Load
Proxy	1 · · · · · · · · · · · · · · · · · · ·	Save
SSH		Delete
Kex		Delete
Host keys		
	Close window on exit:	
Credentials	Always Never Only on	clean exit
About Help	Open	Cancel

Y pulsamos sobre "Open" para conectarnos a Drago mediante la clave RSA.