

Generación de Claves SSH

		G	Generaci	ón d	e Clave	es SSH
TechHelpdesk Instalaciones	FECHA:	25/11/2016	REVISIÓN:	1.1	PAGINA:	Página 2 de 6
Clasificación: Interno						

Revisión/Aprobación				
Elaborado por:	TechHelpdesk Instalaciones			
Revisado por:				
Aprobado por:				

Г

		Histórico de cambios	
Versión	Fecha	Descripción de la acción	
1.0	25/11/2016	Creación del documento.	
1.1	1.1 13/12/2017 Añadido Conversión de claves en formato Putty para su uso en SFTP d		so en SFTP de Linux
		Lista de Distribución	
Fecha		Nombre	Firma



Introducción

En este documento se describe cómo generar las claves de conexión SFTP ssh con el programa PuTTY Key Generator.

Generación de claves SSH con PuTTY Key Generator.

Abriremos el programa *puttygen.exe*, seleccionaremos los Parámetros *SSH2 RSA* (2048) o los correspondientes según Formulario y pulsaremos el botón *Generate*

and the second se	Help		
Key			
Please generate some ran	domness by moving th	ne mouse over the bla	ank area.
Actions			
Actions			Connector
Actions Generate a public/private	key pair		<u>G</u> enerate
Actions Generate a public/private Load an existing private ke	key pair ay file		<u>G</u> enerate Load
Actions Generate a public/private Load an existing private ke Save the generated key	key pair ay file	Save p <u>u</u> blic key	<u>G</u> enerate Load Save private key
Actions Generate a public/private Load an existing private ke Save the generated key Parameters	key pair ay file	Save p <u>u</u> blic key	<u>G</u> enerate Load Save private key
Actions Generate a public/private Load an existing private ke Save the generated key Parameters Type of key to generate: SSH-1 (RSA)	keypair ayfile ⊙ SSH-2 RSA	Save public key	<u>G</u> enerate Load Save private key H-2 DSA



El programa generará una clave pública y otra privada (ppk) que tendremos que salvar.

Are you sure you want to s without a passphrase to pr	save this key rotect it?

La clave Privada se guardará en el Pc

😴 Save private key a	si			X
$\in \mathbb{R}^{2} \times \mathbb{A}$	> Este equipo > Documentos	~ 0	Buscar en Documentos	P
Organizar 🔹 N	ueva carpeta		E •	0
Nombre:				¥
<u>T</u> ipo:	PuTTY Private Key Files (*.ppk)			~
_ipo: ∧ Ocultar carpetas	PuTTY Private Key Files (*.ppk)		Guardar Cance	lar

La clave *Pública* es la que se envía a BME

	Organizar 👻 🛛 N	ueva carpeta			≡ • (
 Decargas Escritorio OneDrive Sitios recientes Escritorio Bibliotecas Documentos Imágenes Música Visica 	👉 Favoritos		Nombre	~	Fecha de modifica Tipo
	Descargas			10 / 1 / 1 / 1 / 1	1.5.5.1.1.2
 OneDrive Sitios recientes Escritorio Bibliotecas Documentos Imágenes Música 	Escritorio			Ningun elemento coincide con	el criterio de busqueda.
Sitios recientes Escritorio Biblioteas Biblioteas Imágenes Música	OneDrive				
Escritorio Bibliotecas Documentos Imágenes Música	📃 Sitios reciente	s			
Escritorio Bibliotecas Documentos Música Música With the transmission With the transm					
Bibliotecas Documentos Imágenes Música	💶 Escritorio				
B Documentos Imágenes Música	词 Bibliotecas				
Imágenes Música ✓ ✓ Im	Documento	s			
Música + < m	🔚 Imágenes				
A CONTRACTOR OF	🚽 Música			S.III.	
Nombre: Nombre que pondremos a la clave publica	Nombre:	Nombre que pondremos a la clave publica			. 17
Tipo: All Files (*.*)	Tipo:	All Files (*.*)			



Conversión de claves en formato Putty para su uso en SFTP de Linux

En el caso de que la pareja de claves se hubieran generado con PuttyGen es necesario exportar la clave privada para su uso en SFTP de Linux siguiendo los siguientes pasos:

Ejecutar Puttygen.exe

Pu	TTY Ke	y Generator			? >
le .	Key (Con <u>v</u> ersions	<u>H</u> elp		
Key No ł	key.				
Actio	ons ierate a	public/private	a key pair		Generate
Actio Gen Loa	ons ierate a d an exi	public/private	a key pair Key file		<u>G</u> enerate Load
Actio Gen Loa	ons ierate a d an exi e the ge	public/privat sting private l merated key	a key pair key file	Save public key	<u>Generate</u> Load Save private key
Actio Gen Loai Sav Para	ons lerate a d an exi e the ge imeters	public/private sting private l merated key	e key pair key file	Save public key	<u>G</u> enerate Load Save private key
Actio Gen Loa Sav Para Type	ons herate a d an exi e the go meters e of key SSH- <u>1</u> (public/private sting private I merated key to generate RSA)	e key pair key file () SSH-2 <u>R</u> SA	Save public key	Generate Load Save private key SH-2 DSA

En el menú seleccionar File->Load private key

PuTT	Y Key Generator			? >
le Ke	y Conversions	Help		
Loa	d private key			
Sav	e public key			
Sav	e private key			
Exit				
Action				
Action	te a public/private	key nair		Generate
Action	ite a public/private	key pair		Generate
Action: Genera Load a	ite a public/private n existing private k	key pair ey file		<u>G</u> enerate Load
Action: Genera Load a Save t	ite a public/private n existing private k ne generated key	key pair ey file	Save public key	<u>G</u> enerate Load Save private key
Actions Genera Load a Save t	i n existing private k ne generated key tters	key pair ey file	Save pyblic key	<u>G</u> enerate Load Save private key
Actions Genera Load a Save t Parama Type o O SS	ite a public/private n existing private k ne generated key tters f key to generate: 1- <u>1</u> (RSA)	• key pair ey file	Save pýblic key	Generate Load Save private key



Seleccionar el fichero de la clave privada (normalmente con extensión .ppk)

Una vez cargada la clave privada seleccionar en el menú Conversions->Export OpenSSH key

e Key	Conversion	Help		
Key	Key Import key			
Public ke Export O		OpenSSH key	ys file:	11.5.50
ssh-rsa +QdvP/ 2qeBUh	Export opensor recy Export ssh.com key		pA2sLS0tqwjAwn Fw/GyOXRax2ajc	nL8HCXHWqhrspY
J8L0Uu	cwGu5Rqr3MT	CBU93YI0COv/pR	kM9al1aM9ezzvyUx/FwF	luzc5Sf11stlL869d V
Key finge	erprint:	ssh-rsa 2048 bd:33	9c:39f5:e5:4a:b4:ca:6d:	e5:be:4e.fb:d3:9d
Key <u>c</u> om	Key comment: rsa-key			
Key p <u>a</u> s:	sphrase:			
C <u>o</u> nfirm (bassphrase:			
Actions				
Generate	e a public/privat	e key pair		<u>G</u> enerate
Load an	existing private	key file		Load
Save the	Save the generated key		Save p <u>u</u> blic key	Save private key
Paramete	ers			
T	key to generate	SSH-2 B	SA OSS	H-2 DSA
O SSH-	.T (U2A)	0	· · · · · · · · · · · · · · · · · · ·	

Responder "Si" si se desea guardar la clave privada sin contraseña.



Especificar nombre de fichero de salida (es indiferente la extensión del fichero) y guardar.

Dicho fichero exportado es la clave privada que se ha de especificar en la conexión SFTP de Linux.

Si se desea comprobar, el fichero exportado ha de comenzar y terminar con las etiquetas (BEGIN RSA PRIVATE KEY) y (END RSA PRIVATE KEY) y la clave privada comienza normalmente con las letras (MIIE) como por ejemplo:

```
-----BEGIN RSA PRIVATE KEY-----
MIIEoQIBAAKCAQEArcP+QdvPAzSqT0wf
tawiAwmI.8HCXHWahrspY2geBUhOgVPA0
qAOlDiOchuiOGXeTE5i5f8q1s31+i(
-----END RSA PRIVATE KEY-----
```