

SSH Key Generation





REVIEW/APPROVAL	
Made by:	TechHelpdesk Instalations
Reviewed by:	
Approved by:	

		CHANGES IN THE HISTORY
VERSION	DATE	ACTION DESCRIPTION
1.0	25/11/2016	Creation of the document
1.1	13/12/2017	Added Conversion of keys in Putty format for use in Linux SFTP

	DISTRIBUTION LIST	
DATE	NAME	SIGN



Introduction

In this document is explained how generate SFTP SSH connection keys with PuTTY Key Generator Software.

SSH Key Generation with PuTTY Key Generator

Firstly, we will open program puttygen.exe and select parameters **SSH2 RSA (2048)** or the corresponding ones according to Form and we will click **Generate button**.

e <u>K</u> ey Con <u>v</u> ersions <u>I</u>	Help		
Key			
Please generate some rando	mness by moving th	he mouse over the bla	ank area.
A			
Actions			
Actions Generate a public/private ke	sy pair		Generate
			<u>G</u> enerate Load
Generate a public/private key			Load
Generate a public/private ke		Save pyblic key	
Generate a public/private key		Save public key	Load
Generate a public/private key Load an existing private key Save the generated key		Save public key	Load
Generate a public/private ke Load an existing private key Save the generated key Parameters			Load

The program will generate a public key and another private (ppk) that we will have to save.





Private Key will be saved in the computer:

← → • ↑ 🖪	> Este equipo > Documentos	~	Ö	Buscar en Documentos	م
Organizar 👻 N	ueva carpeta			E •	0
Nombre:	1				~
Tipo:	PuTTY Private Key Files (*.ppk)				*

Public Key has to be sent to BME:

rganizar 👻 Nueva carpeta			~	100	
Favoritos	<u>^</u>	Nombre		Fecha de modifica.	Tipo
🍓 Descargas	E	Nir	ngún elemento coincide c	on el criterio de búsqueda.	
Escritorio					
OneDrive					
Sitios recientes					
Escritorio					
🕞 Bibliotecas					
Documentos					
🔛 Imágenes					
🚽 Música		1	m		
Nombre: Nombre que pondremos a la clave	e publica				
Tipo: All Files (*.*)					



Conversion of keys in Putty format for use in Linux SFTP

In case of the pair of keys have been generated with PuttyGen it s necessary export public key for use it in Linux SFTP following the next steps:

Execute Puttygen.exe:

ru.	ITTY Ke	y Generator			? >
ile	Key (Conversions	Help		
Key	,				
No	key.				
Acti	ions				
		public/private	key pair		Generate
Ger	nerate a	public/private sting private k			<u>G</u> enerate Load
Ger Loa	nerate a ad an ex			Save pyblic key	
Ger Loa Sav	nerate a ad an ex	sting private k		Save pyblic key	Load
Ger Loa Sav Pan Typ	nerate a ad an ex ve the gr ameters	sting private k enerated key r to generate:			Load

In Top Menu select File -> Load private key

PuTTY Ke	ey Generator			?	×
le Key	Conversions	Help			
Load p	rivate key				
Save p	ublic key				
Save pr	rivate key				
Exit					
Actions					
	a public/private	key pair		Generat	e
Generate a	a public/private sisting private k			<u>G</u> enerat	e
Generate a Load an ex			Save pyblic key	Reserves	A
Generate a Load an ex	isting private k enerated key		Save public key	Load	A
Generate a Load an ex Save the g Parameters Type of ke	isting private k enerated key			Load	A

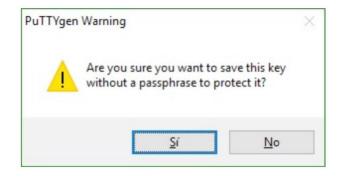


Select private key file (usually with extension .ppk)

Once private key is loaded, select in menú Conversions -> Export OpenSSH key.

ile Key	(ey Generator Conversions				1
Key	Import	key			
Public ke	Export	OpenSSH key	ys file:		
ssh-rsa A +QdvPA	Export	ssh.com key	pA2sLS0tqwjAwn	L8HCXHWqhrspY	^
2qeBUh0 +rwvXm1 J8L0Uuc	DLPeX4oOi/C wGu5Rqr3MT(rZPXdEtVa8dN5mGDlr CBU93Y10COv/pRkM9	mgZxj7lidO5flb1xPHQ al1aM9ezzvyUx/FwH	nDmJeCrQPC lail9z2xu0sqJzRpw łuzc5Sf11stlL869d	~
Key finger	print:	ssh-rsa 2048 bd:33:9c:	39f5:e5:4a:b4:ca:6d	e5:be:4efb:d3:9d	
Key com	nent:	sa-key-20171213			
Key pass	ohrase:				
Confirm p	assphrase:				
Actions					
Generate	a public/privat	e key pair		<u>G</u> enerate	
Load an e	existing private	key file		Load	
Save the	generated key	[Save public key	Save private ke	y
Parameter	rs				
	ey to generate:	SSH-2 RSA	Oss	H-2 DSA	
Type of k	(INSA)	C. C. C. L. L. L.			

Answer "Yes" to save public key without password.



Specify output file name (don't worry about file extension) and save. That exported file is private key that has to be provided in SFTP Linux connection.



If you want to check, exported file has to begin and end with labels (BEGIN RSA PRIVATE KEY) and (END RSA PRIVATE KEY), and private key usually begins with letters (MIIE) as follows:

----BEGIN RSA PRIVATE KEY-----MIIEoQIBAAKCAQEArcP+QdvPAzSqT0wf tawiAwmL8HCXHWahrspY2geBUh0gVPA0

qAOlDiOchuiOGXeTE5i5f8q1s31+i(-----END RSA PRIVATE KEY-----

This material has been prepared by Bolsas y Mercados Españoles, Sociedad Holding de Mercados y Sistemas Financieros S. A. (BME), its subsidiaries, affiliates and/or their branches (together, "BME") for the exclusive use of the persons to whom BME delivers this material. This material or any of its content is not to be construed as a binding agreement, recommendation, investment advice, solicitation, invitation or offer to buy or sell financial information, products, solutions or services. The information does not reflect the firm positions (proprietary or third party) of the entities involved in the Spanish Securities Market. BME is under no obligation to update, revise or keep current the content of this material, and is subject to change without notice at any time. No representation, warranty, guarantee or undertaking – express or implied – is or will be given by BME as to the accuracy, completeness, sufficiency, suitability or reliability of the content of this material.

The opinions presented are theoretical and, therefore, the content hereof is intended for informational purposes only and should not be used for portfolio or asset valuations, or as the basis for any investment recommendations. Neither contributing Entities, nor Bolsas y Mercados Es pañoles, Sociedad Holding de Mercados y Sistemas Financieros S.A. (BME) nor any of its subsidiaries, accept responsibility for any financial loss or decision made based on the information contained in this material. In general, neither Bolsas y Mercados Españoles, Sociedad Holding de Mercados y Sistemas Financieros S.A. (BME) nor any of its subsidiaries, accept responsibility for any financial os or decision made based on the information subsidiaries, nor the contributing Entities, their directors, representatives, associates, subsidiaries, managers, partners, employees or advisors accept any responsibility for this information or unauthorised use of the same.

This material is property of BME and may not be printed, copied, reproduced, published, passed on, disclosed or distributed in any form without the express prior written consent of BME.

2023 Bolsas y Mercados Españoles, Sociedad Holding de Mercados y Sistemas Financieros S. A. All rights reserved.

BME

Plaza de la Lealtad,1 Palacio de la Bolsa 28014 Madrid

