Creating and Using SSH Keys from a Computer Running Microsoft Windows

SSH keys are what you will use to establish an encrypted connection over the network, e.g. the internet, between your system and a remote machine. The default type of key to generate is RSA which is good for most purposes. RSA is universally supported among SSH clients. Note that EdDSA performs much faster and provides the same level of security with significantly smaller keys. In general, though, for what you need to do, RSA encryption should just work.

Section I. Install PuTTY

To create and use SSH keys on a device running Microsoft Windows, you need to first download and install both PuTTY and PuTTYgen on that device. PuTTY is the utility used to connect your to a remote desktop or server through SSH, and PuTTYgen is the utility used to create SSH keys. On <u>the PuTTY website</u>, download the .msi file in the **Package files** section at the top of the page, under **MSI ('Windows Installer')**. Next, install it on your local computer by double clicking it and using the installation wizard.

After the programs are installed, start the PuTTYgen program through your Start Menu or by tapping the Windows key and typing puttygen. The PuTTY key generation program will launch and open in a window.

😴 PuTTY Key Generator			? ×
File Key Conversions Help			
Key No key.			
Actions Generate a public/private key pair Load an existing private key file			Generate
Save the generated key		Save public key	Save private key
Parameters Type of key to generate:	OECDSA	OEdDSA	() SSH-1 (RSA)
Number of bits in a generated key:	0	0	2048

Section II. Create a Set of SSH Keys

Click the button [Generate] to begin the process of generating an RSA set of keys. By "set" this means you will generate two keys, a private key and a public key. The public key is a key that gets installed on the remote host that you want access to. The private key is saved on the device that you are using and is not to be moved, shared or given to anyone, whence its name "private".

After you click [Generate] you will be prompted to move the mouse around in order to generate some randomness that will be used in the creation of your keys.

PuTTY Key Generator		? >
e Key Conversions Help		
Key Please generate some randomness by moving the mouse ov	rer the blank area.	
		Generate
Generate a public/private key pair		Generate
Generate a public/private key pair Load an existing private key file	Save public key	
Generate a public/private key pair Load an existing private key file Save the generated key	Save public key	Load
Actions Generate a public/private key pair Load an existing private key file Save the generated key Parameters Type of key to generate:		Load

After moving the mouse around for a short while, the program will create your keys and display something as follows.

📍 PuTTY Key Genera	tor			?	
e Key Conversion	s Help				
Key					
Public key for pasting	into OpenSSH authoriz	ed_keys file:			
JcLAC5JxH1bwh4Hi8 +2ig5NzeY1Lm31Ha	LxwK2akT/ZXsB2qiQC betiU52/6J7ARN491RS	zHckT4cx+e6WiaBPt y4DdQG9oLQl6s8yvu			-
Key fingerprint	ssh-rsa 2048 SHA256	WLN43ZNg2pSdSR4	4/Qs6B6shQgEX0/xvuseu3/0	QYNsiw	
Key comment	rsa-key-20220829				
Key passphrase:					_
Confirm passphrase:					
Actions					
Generate a public/priv	vate key pair			Generate	
Load an existing priva	te key file			Load	
Load an existing priva Save the generated k			Save public key	Load Save private key	
Save the generated k			Save public key		
	ey	OECDSA	Save public key		

Notice that the public key is displayed at the top and that several other fields have been added. One notable field is the "Key Passphrase". Some facilities require its users to set a passphrase whereas others leave it to you to decide. A passphrase is like a password that you must enter

each time you use these keys. For now, we will choose to skip using a pass phrase and proceed to save our keys into files on our local system.

Click [Save public key] to save the public key to a file. This is the file that you will install on a remote host that you want to connect with using SSH keys rather than typing a password. A Windows save file box opens. You can create a folder called "PuttyKeys" or whatever you want to name it or simply save it to a location you will not forget and will not delete.

- → v ↑ → This PC > Documents > PuttyKeys			v 0	,○ Search P	PuttyKeys	
A North						
					- E	
This PC Name This PC Name To show the set of the set	Date modified No items mat	Type ch your search.	Size			
File name: public-key-20220829						
Save as type: All Files (*.*)						

Once you save your public key, you need to save your private key. Click on [Save private key].

PuTTY Key Gener	ator			?	×
e Key Conversion	ns Help				
Key					
Public key for pasting	g into OpenSSH authoriz	ed_keys file:			
JcLAC5JxH1bwh4H +2ig5NzeY1Lm31Ha	i5LxwK2akT/ZXsB2qiQC aoetiU52/6J7ARN491RS	zHckT4cx+e6WiaB sy4DdQG9oLQl6s8y			
Key fingerprint	ssh-rsa 2048 SHA256	WLN43ZNg2pSdS	R4/Qs6B6shQgEX0/xvuseu3/	QYNsiw	
Key comment	rsa-key-20220829				
Key passphrase:					_
Confirm passphrase					
Actions					
Generate a public/pr	ivate key pair			Generate	
Load an existing priv	ate key file			Load	
Save the generated	key		Save public key	Save private key	
Parameters					
Type of key to gener RSA	rate: ODSA	OECDSA	OEdDSA	OSSH-1 (RSA)	

After you click [Save private key], if you did not set a passphrase, then you will be asked "Are you sure you want to save this key without a passphrase to protect it?

Key				
Public key for pasting	into OpenSSH	authorized, keys file:		
ssh-rsa AAAAB3NzaC1yc2E JcLAC5JxH1bwh4Hit +2ig5NzeY1Lm31Ha	AAAADAQABA 5LxwK2akT/ZXs oetiU52/6J7AR	AABAQCEQsQXNZAqO4t7G0Z7B7DcS6m2XXXZb6kdWasXF B2qiQC2HckT4cx+e6WiaBPhxxm36Y9Pqu N491RSy4DdQG9oLQl6s8yvuyd FV9pAHtey0WAFiB92njotdgVqWFfH+0NlfVSu3r0dYuTbWTj	MT9wZF/36y54yjFk2T	,
Key fingerprint	ssh-rsa 2048	SHA256:WLN43ZNg2pSdSR4/Qs6B6shQgEX0/xvuseu3/QYN	siw	
Key comment	rsa-key-2022	0829		
Key passphrase:				
Confirm passphrase:				
Actions		PuTTYgen Warning ×		
	vate key pair		Generate	
Generate a public/pri	rate ney pan			
		Are you sure you want to save this key without a passphrase to protect it?	Load	
Load an existing priva	ate key file	Are you sure you want to save this key without a passphrase to protect it?	Load Save private key	
Load an existing priva Save the generated k	ate key file	without a passphrase to protect it?		
Generate a public/pri Load an existing priva Save the generated k Parameters Type of key to genera @ RSA	ate key file key			

If you don't want to use a passphrase, then click [Yes] to close out the message box and proceed to save the file. Note that the file is save with a PuTTY Private Key (*.ppk) extension.

😴 Save private key as:				×
$\leftarrow \rightarrow \checkmark \uparrow$ 🖡 > This PC > Documents > PuttyKeys			・ じ	arch PuttyKeys
Organize • New folder				≣ • 👔
 This PC 3D Objects Desktop Documents Downloads Music Pictures Videos Windows 10 (C:) Google Drive (G: 	Date modified No items mat	Type	Size	
File name: private-key-20220829 Save as type: PUTTY Private Key Files (*.ppk)			Save	e Cancel

To alleviate some frustration and pain on your part, we note that the format of the public key file is not very user friendly to the Linux world. So for now we are going to save the public key (not the private key!) again but in a text file. From the PuTTYgen utility you will notice the public key is displayed in a box at the top of that utility.

🥐 PuTTY Key Genera	itor				?	×
le Key Conversion	ns Help					
Key						
Public key for pasting	into OpenSSH author	rized_keys file:				
ssh-rsa		QCEQsQXNZAqO4t7G	077870-56-077775	6kdWaeYEMT9w7E/	260540642	^
JcLAC5JxH1bwh4Hi	5LxwK2akT/ZXsB2qiC	CzHckT4cx+e6WiaBPI	hvxmf36Y9Pqu	okurrashi witswzi j	збузнур ка	
		RSy4DdQG9oLQl6s8yvi AHteyOWAFiB92njotdg		dYuTbWTjgP		~
Key fingerprint		56:WLN43ZNg2pSdSR				_
Key comment	rsa-key-20220829		,			_
	15a-Key-20220025					_
Key passphrase:						
Confirm passphrase:						
Actions						
Generate a public/pri	ivate key pair			Ge	nerate	
Load an existing priva	ate key file			L	.oad	
Save the generated	key		Save public key	Save p	orivate key	
Parameters						
Type of key to gener	ate: ODSA	ECDSA	OEdDSA	Ossi	I-1 (RSA)	
			0	0		

Click on that window to highlight or select everything in that box. Copy and paste that information to Notepad. It is important to note that everything that is being copied is just one very long line. It is not two or three lines, but a single line. Make certain you paste it into Notepad and save it as such.

🧾 *Un	ntitled - Note	pad							_		×
File E	dit Format	View	Help								
ssh-r AAAAB kT/ZX +hW6s	sa 3NzaC1yc2 sB2qiQCzH Znl/jr0Z7	EAAAA lckT4c PqZwi	Help DAQABAAABAQCEQsQXh x+e6WiaBPhvxmf36Y3 oj3CLCGdvGJFVepAHt UtT9PU3CKAAxSBsNNE	9Pqu+2ig5NzeY1L tey0WAFiB92njot	m31HaoetiU dgVqWFfH+OM	2/6J7ARN491R IfVSu3r0dYuT	Sy4DdQG9 bWTjgP	oLQI6s8yvuyd			K2a
					L		100%	Windows (CRLF)		-8	

Now save this file to the same location where you previously saved your public and private keys.

Save As							×
\leftarrow \rightarrow \checkmark \uparrow 📜 \Rightarrow This PC \Rightarrow Documents \Rightarrow Putty	/Keys	~	Ō	Ņ	Search Putt	yKeys	
Organize 👻 New folder							?
 This PC 3D Objects Desktop Documents Downloads Music Pictures Videos 	ţ	Date mod			Туре		Size
5 Windows 10 (C:) Y <							>
File name: public-key-20220829-for-Linux							~
Save as type: Text Documents (*.txt)							~
∧ Hide Folders	Encoding:	UTF-8	~		Save	Can	cel

Section III. Install your Public Key on the Remote Host

If you can SSH to the host then you can copy and paste that PUBLIC key into a file under your home account as

~/.ssh/authorized keys

or

/home/your_username/.ssh/authorized_keys

where the symbol "~" represents a shortcut for "/home/your username".

If the hidden .ssh sub-directory does not exist, then you need to create it manually as

\$ cd
\$ mkdir .ssh
\$ chmod 700 .ssh
\$ cd .ssh
\$ touch authorized_keys
\$ chmod 600 authorized_keys

You will then copy/paste the public key into this "authorized_keys" file.

Section IV. Configure a PuTTY Session to Use the Key file

Launch the PuTTY utility program. Enter

Host Name or IP Address:remote-computer.cs.vassar.edu(or the IP address)Saved Sessions:computerPort:22

NOTE: Here the default port for SSH is 22, but it may be different at different sites.

<mark>⊫</mark> Session	^	Basic options for your PuT	TY ses	sion
⊡ Logging ⊡ Terminal Keyboard		Specify the destination you want to Host Name (or IP address) remote-computer-name-OR-IP-Addr		Port
Bell Features		Connection type:	ess	22
Appearance Behaviour Translation ⊕ Selection		SSH Oserial Other: Load, save or delete a stored sessio Saved Sessions remote-computer	n	
Colours		Default Settings	^	Load
── Proxy ⊟ SSH Kex		к. к.	~	Save Delete
Proxy	~	Close window on exit: Always Never Only		

Next, under "Connection" select "Data" and enter your "username" which is the name of the account you will use to login with to the remote computer.

RepuTTY Configuration ? Х Category: - Session Data to send to the server ^ Logging Login details - Terminal Auto-login usemame your-login-name Keyboard Bell When usemame is not specified: Features Prompt Ouse system usemame (dfrey) . Window Terminal details Appearance --- Behaviour Terminal-type string xterm - Translation Terminal speeds 38400,38400 . Selection --- Colours Environment variables - Connection Variable Add Data - Proxy Value Remove SSH Kex - Host keys - Cipher + Auth TTY X11 ¥ About Help Open Cancel

Auto-login username: your_loginname

Now, under "Connection" click on "SSH" and then "Auth". Click the [Browse] button and navigate to where you saved your private key in a key file. Select the private key file.



Finally, go back to the "Sessions" category and click [Save] so that this configuration will be saved and you won't have to repeat these steps!

🕵 PuTTY Configurat	ion		? ×
Category:			
 Session Logging Terminal Keyboard 	^	Basic options for your PuTTY's Specify the destination you want to conn Host Name (or IP address)	
Bell Features		Connection type:	
Appearance Behaviour Translation Selection		SSH Oserial Other: Telr Load, save or delete a stored session Saved Sessions remote-computer	
Colours Connection Data Proxy		Default Settings	Load Save
SSH Kex Host keys Cipher			Delete
⊕ Auth TTY X11	~	Close window on exit: Always O Never Only on	clean exit
About	Help	Open	Cancel

Now when you launch PuTTY all you have to do is locate under your saved sessions the session you want to use, click on the name once to select it and then click [Load] and then click [Open]. A shorter way to do this is to just double-click on the session name from the list of sessions and that will start a remote SSH session.

References

SSH Keys

https://www.ssh.com/academy/ssh-keys

What are SSH Keys?

https://www.appviewx.com/education-center/what-are-ssh-keys/

How to Create SSH Keys with PuTTY

https://docs.digitalocean.com/products/droplets/how-to/add-ssh-keys/create-with-putty/