∧ inera

Instruktioner för hur du skapar ett SSH-nyckelpar

Revisionshistorik

VERSION	DATUM	FÖRFATTARE	KOMMENTAR
1.0	2021-02-18	Sil Teknik	Revision. Inlagd i nytt word-dokument.

Skapa ett SSH-nyckelpar

Vid inloggning till Sil SFTP använder ni en SSH-nyckel. Nedan förklarar vi hur ni skapar ett SSH-nyckelpar.

Den ena nyckeln som skapas är hemlig och kommer att vara er privata nyckel. Den privata nyckeln används senare av er för att logga in mot vår SFTP-server.

Den andra nyckeln som skapas är er publika nyckel. Denna nyckel anger ni i ansökan till oss och det är även denna nyckel som vi kommer att godkänna på vår sida.

Windows

- 1. Ladda ner programmet "<u>PuTTYgen</u>".
- 2. Starta "puttygen.exe".
- 3. Se till att alternativet "**RSA**" är valt, fyll i värdet "**4096**" och klicka sedan på knappen "**Generate**".

[∧] inera

😴 P	uTTY I	Key Generator				?	×
File	Key	Conversions	Help				
N	ey o key.		•				
G	enerate	a public/private	key nair			Generate	
Ĭ.		a public/private	NCy pair			Generate	
L	oad an (existing private ke	ey file			Load	
S	ave the	generated key		Save	public key	Save private ke	ey 🛛
Pa	aramete	rs					
T N	vpe of k RSA umber o	ey to generate: DDSA f bits in a genera	ted key:	6A	○ Ed25519	○ SSH-1 (R 4096	5A)

4. SSH-nyckelparet slumpas fram genom att ni (tro det eller ej) rör på muspekaren.

Please generate some randomness by moving the mouse over the blank area.							

5. I den stora, rödmarkerade rutan (se nedan) visas er *publika* nyckel. Denna nyckel anger ni i ansökan till oss och det är även denna nyckel som vi kommer att godkänna på vår sida.

Se även till att klicka på knappen "**Save private key**" för att spara ner er *privata* nyckel. Denna används senare av er för att logga in mot vår SFTP-server.

[∧] inera

PuTTY Key Generator ?							
File Key Conversion	ns Help						
Key Public key for pasting in ssh-rsa AAAAB3NzaC1yc2EA WbJR5GKdDruMzQIP +eN0ZFWzEiAmKAqf0 cwi2E5wR0GH lmUPR	nto Open SSH authori: AAABJQAAAgEApae 80A+b9bITNe2i SwLnvV0XXQuWDA/ Kmap82a7DaDum ID4	zed keys file: DIG9wLMU6pp7rGbk5k CoyKOPuPLJfaBfBOsoo 2do /10rocoKayDb52T	JgHlb3iqmAzGQz0				
Key fingerprint:	ssh-rsa 4096 43:af:4	e:91:64:a4:7e:ba:5a:97	:1e.f1:78:4d:6f:2a				
Key comment:	rsa-key-20210218						
Key passphrase:							
Confirm passphrase:							
Actions							
Generate a public/priva	ate key pair		Generate				
Load an existing private	e key file		Load				
Save the generated ke	у	Save public key	Save private key				
Parameters							
RSA O	SA ○ECI	OSA 🔿 Ed25519	SSH-1 (RSA)				
Number of bits in a gen	erated key:		4096				

Linux

I nedanstående exempel förutsätter vi att ni använder pakethanteraren apt (som bl.a. är en del av Ubuntu).

- Ladda ner den senaste informationen om tillgängliga paket: user@server:~\$ sudo apt-get update
- Installera paketet "openssh-client": user@server:~\$ sudo apt-get install openssh-client
- Generera ett SSH-nyckelpar: user@server:~\$ssh-keygen -t rsa -b 4096
- 4. Tryck "Enter" när texten "Enter file in which to save the key (/home/user/.ssh/id_rsa)." visas.
- 5. Tryck "**Enter**" när texten "*Enter passphrase (empty for no passphrase).*" visas.
- 6. Tryck "Enter" när texten "Enter same passphrase again." visas.
- Gå till ".ssh"-katalogen som skapats i er användares hemkatalog (där "username" ersätts med ert användarnamn): user@server:~\$ cd /home/username/.ssh



 Lista alla filer i katalogen: user@server:~/.ssh\$ ls -al

user@server	`: ^	-/.ssł	n\$ 1s	-al					
total 16									
drwx	2	user	user	4096	Sep	22	16:55		
drwxr-xr-x	4	user	user	4096	Sep	22	16:54		
-rw	1	user	user	3243	Sep	22	16:55	id_rsa	
-rw-rr	1	user	user	737	Sep	22	16:55	id_rsa.pub	

- 9. Filen "id_rsa" är er *privata* nyckel och "id_rsa.pub" är er *publika* nyckel.
- 10. Titta hur den publika nyckeln ser ut: user@server:~/.ssh\$ tail id_rsa.pub

user@server:~/.ssh\$ tail id_rsa.pub

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQCu8tZm+aHkOKUVtT375ENdJPy6tKBTFV9Mb8JsN DHGOYupc+xTFZIigZQxfhxhxNRkXm6UBb4cidYiq0hGyj7YGGNP6I/PevDutAr6ZN4bWb52LfmnL1 j73oqxjie4edIvUahpa7uDVcQL+tMmKr4LKxTHG0DiQ0TX4sW9kSbQ/GYW1715mxfrOxdRwAWrgmc yha+t6x97jzd7bKdJZVOpEPa99IIweayTrePh4KtJPR4uRrEriXCvi5W5cHNdj1sAGTPzuFx82NwZ 94G7vODJ0CbCalMWtHKLwcDYsu4HGKTgekqbp1grnA6jTnQnOfjfYFvqFKRI2hiuulYkiDHSj9JGY IYevbV+GFiG5qt9hO2ZIGbk7M70+Sta9wx42W8C4IXis0x7cLhx9EUFF8R+j18I6wyu1UWL5QuyZS mQ6vERGI9iVED3dC6tHdTB7o9hQIvySqHlSarV11zwmwn+XjQMW9wFvvcCb+6rz1+envTiHHhN88F iB9Z6WFINbTE35rWUFkO/z9AmIb5SBAEDGcnXvJpDPeVb8Txo0TToMW6viP2UWtgUG1UAj76vHZfu aKrCracHCB9zqP44SAg7M1W6ImQ4mpWj5cYwxjF1fEmYXiZCEOoHOqFrocsptBjs79k/TRIDR/Y/P nBwRt9NDNeWZqg7rNSP191jjQGZLQ== user@server user@server:~/.ssh\$

- 11. Kopiera den *publika* nyckeln och bifoga denna i ansökan till oss.
- 12. Spara den *privata* nyckeln (filen "**id_rsa**") för att kunna ansluta till SFTP-servern när vi senare godkänt er ansökan.