Wykorzystanie certyfikatów

written by archi | 22 kwietnia 2021

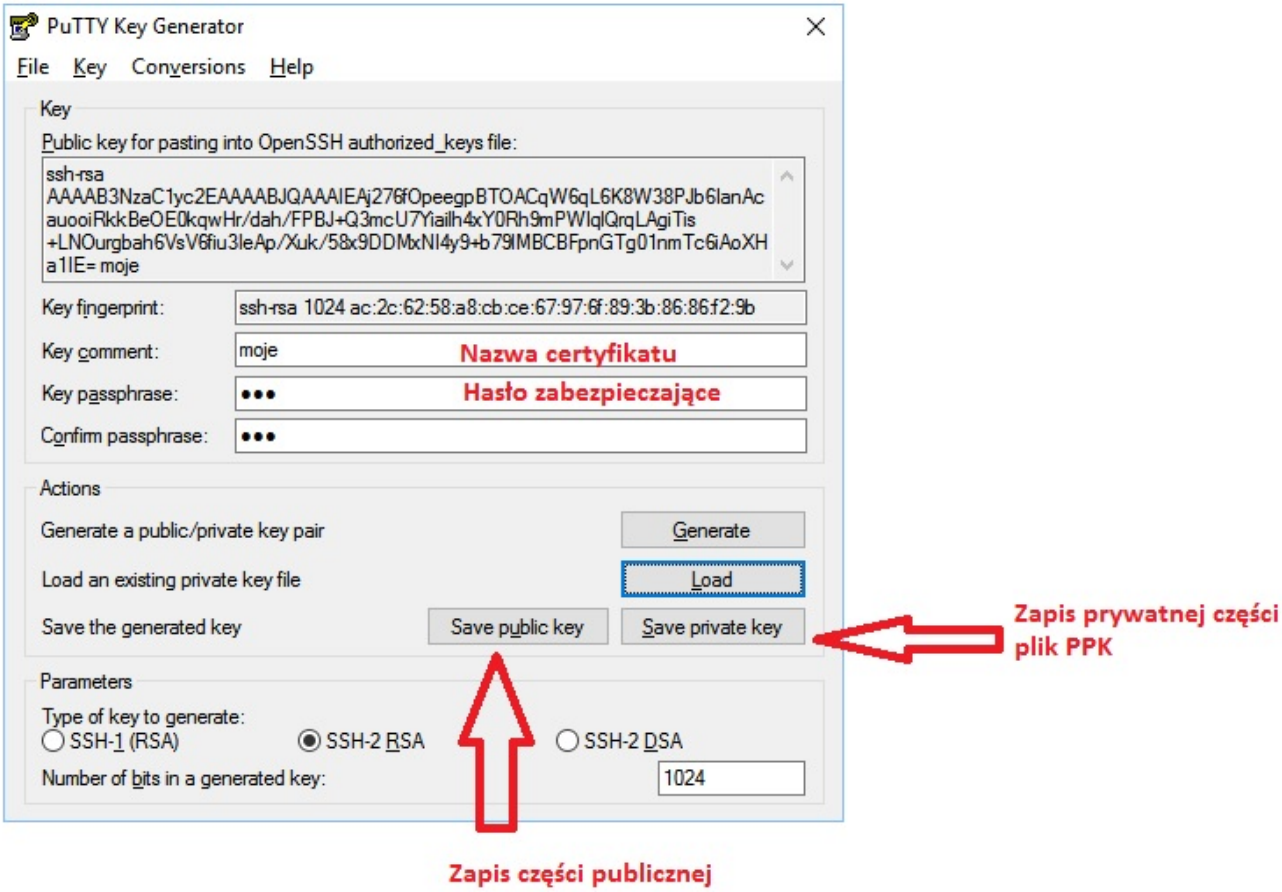
Ze strony http://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html pobieramy oprogramowanie

a) putty.exe

b) pageant.exe

c) puttygen.exe

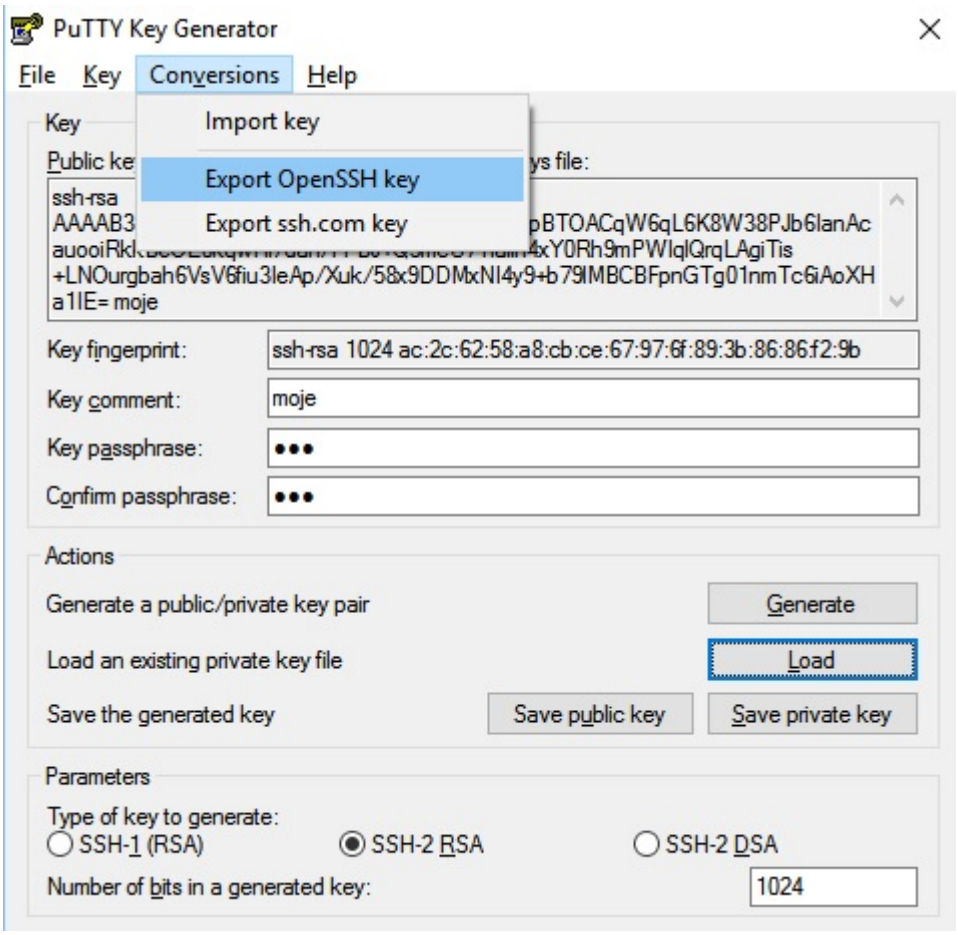
2. przy pomocy „`puttygen.exe`” generujemy certyfikat RSA (część publiczną i prywatną)



3. nazywamy certyfikat i tworzymy hasło zabezpieczające klucz prywatny

4. zapisujemy klucz prywatny i publiczny na dysku

4a. Jeśli chcemy wykorzystać aplikacje na smartphone JuiceSSH to przyda się wersja klucza prywatnego w wersji OpenSSH



5. Plik publicznej części certyfikatu poprawiamy do formatu:

`ssh-rsa AAAAB3NzaC1y[…]FCcR8= moje`

gdzie:

ssh-rsa to typ

moje to nazwa certyfikatu

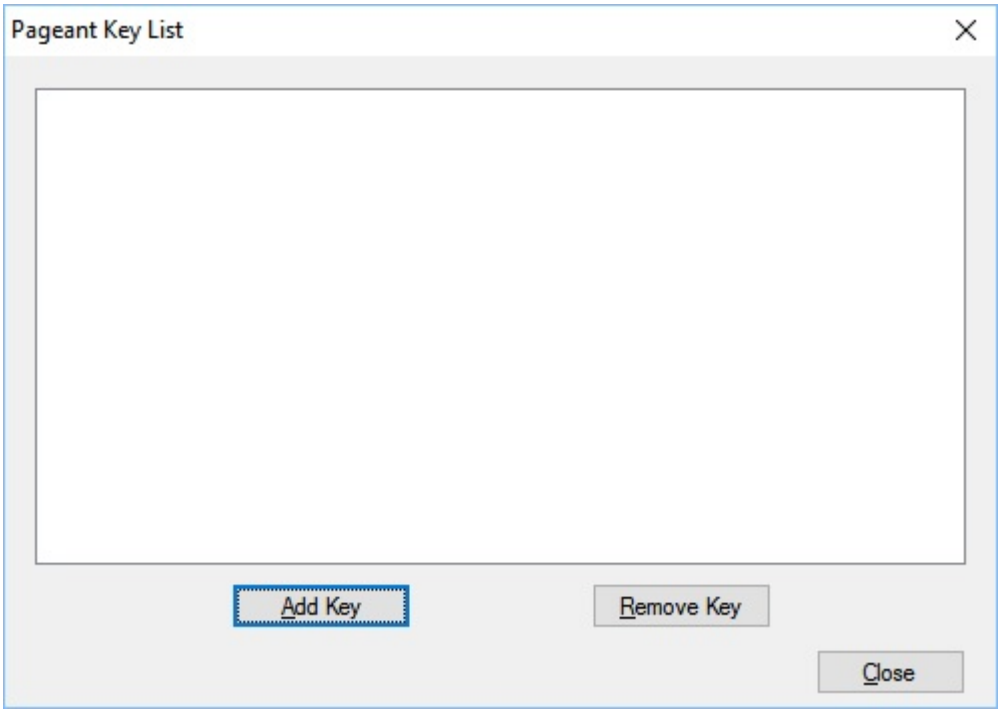
6. poprawioną wersję części publicznej certyfikatu wgrywamy na serwer do konta, na które chcemy się logować bez hasła (np. przez WinSCP).

W przypadku konta „root” w katalogu `/root` tworzymy folder „`.ssh`” a w nim plik „`authorized_keys`” i wklejamy tam zawartość poprawionego

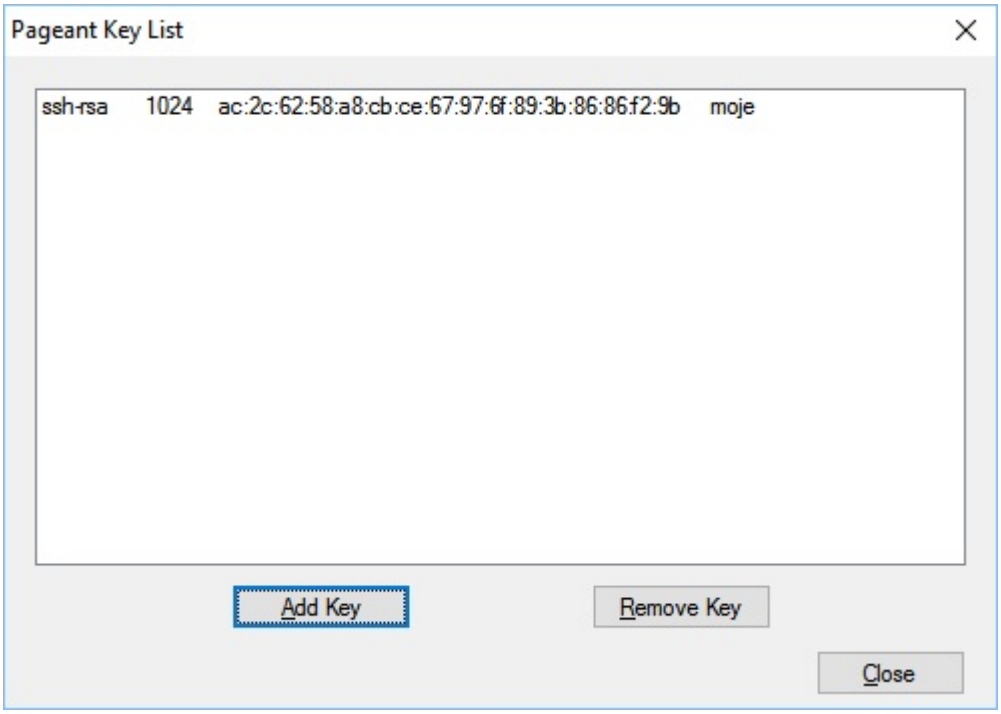
certyfikatu publicznego.

7. zmieniamy uprawnienia na folderze „`.ssh`” oraz pliku „`authorized_keys`” na „400” (r– — —) i właścicielem pliku musi być root i grupa root

8. na stacji uruchamiamy program `pagent.exe` (odpali się w tray, koło zegarka)

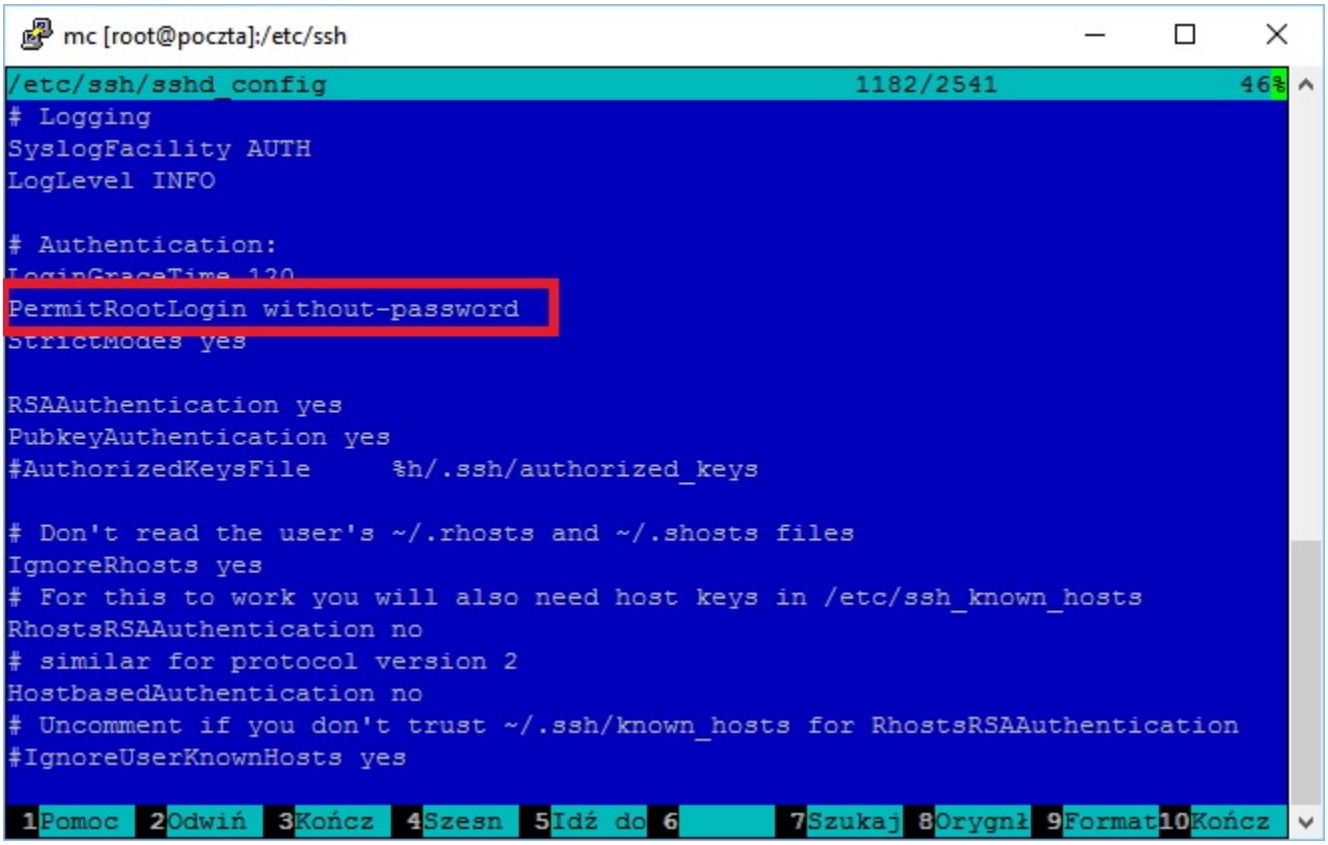


i dodajemy nasz klucz podając hasło które ustawiliśmy do klucza



9. możemy się już logować na serwer bez użycia hasła bezpośrednio na konto ROOT

10. Dodatkowo powinniśmy zabezpieczyć serwer i konto root w konfiguracji SSH aby nie można było logować się na nie przy pomocy hasła tylko przy pomocy certyfikatu


mc [root@poczta]:/etc/ssh
/etc/ssh/sshd_config 1182/2541 46%
Logging
SyslogFacility AUTH
LogLevel INFO
Authentication:
LoginGraceTime 120
PermitRootLogin without-password
StrictModes yes
RSAAuthentication yes
PubkeyAuthentication yes
#AuthorizedKeysFile %h/.ssh/authorized_keys
Don't read the user's ~/.rhosts and ~/.shosts files
IgnoreRhosts yes
For this to work you will also need host keys in /etc/ssh_known_hosts
RhostsRSAAuthentication no
similar for protocol version 2
HostbasedAuthentication no
Uncomment if you don't trust ~/.ssh/known_hosts for RhostsRSAAuthentication
#IgnoreUserKnownHosts yes
1Pomoc 2Odwiń 3Kończ 4Szesn 5Idź do 6 7Szukaj 8Orygnł 9Format10Kończ