

Instrukcja generowania kluczy SSH na potrzeby połączenia z serwerem SFTP PSG

Spis treści

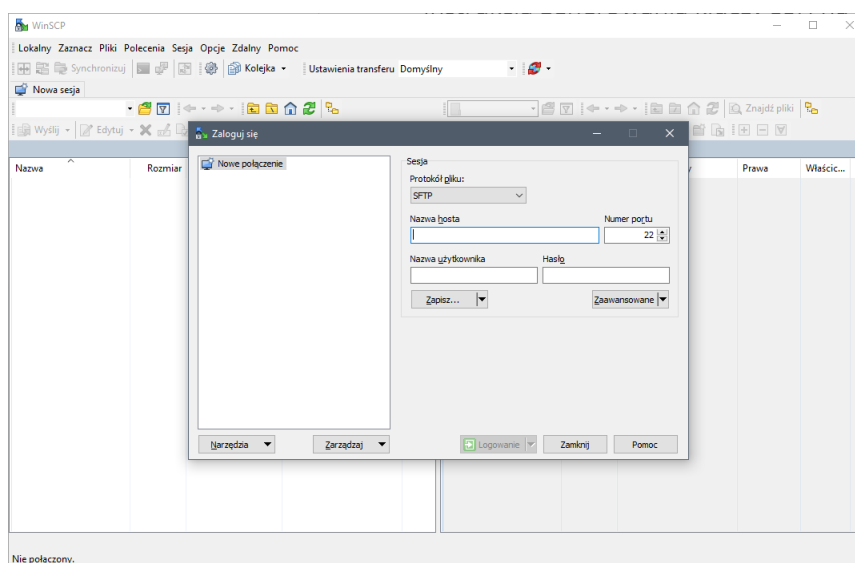
Wstęp	1
Generowanie kluczy SSH	1
Konfiguracja połączenia do SFTP	4
Nawiązywanie bezpiecznego połączenia.....	6

Wstęp

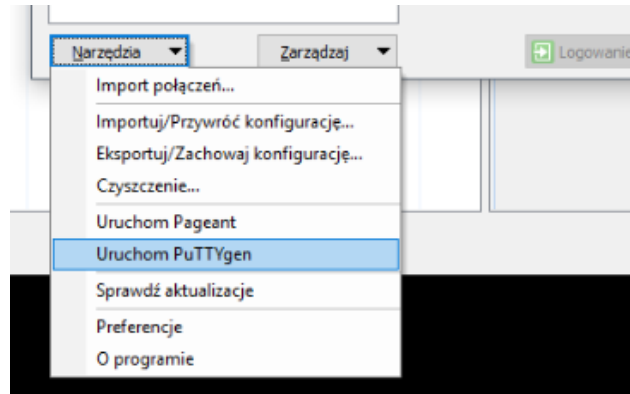
Instrukcja opisuje proces generowania kluczy prywatnego i publicznego niezbędnego do nawiązania szyfrowanego połączenia z serwerem PSG. Opis bazuje na darmowym kliencie WinSCP, którego można pobrać ze strony producenta: <https://winscp.net/eng/download.php>

Generowanie kluczy SSH

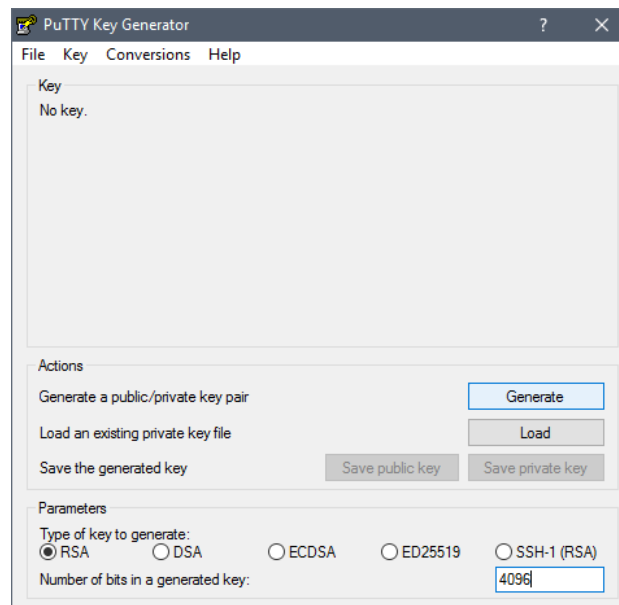
1. Pobieramy i instalujemy klienta WinSCP, o ile nie jest dostępny w naszym systemie. Następnie uruchamiamy go:



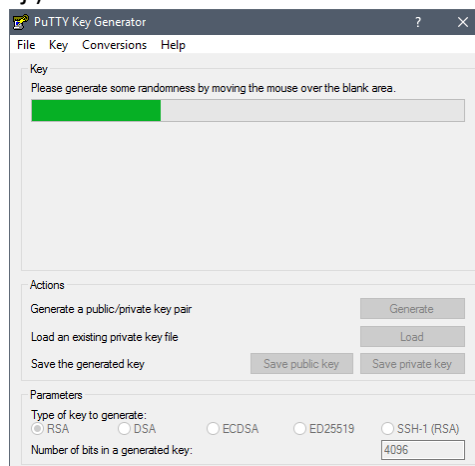
2. Generujemy parę kluczy: prywatny oraz publiczny – w tym celu rozwijamy menu *Narzędzia* widoczne w lewym dolnym rogu ekranu i wybieramy *Uruchom PuTTYgen*:



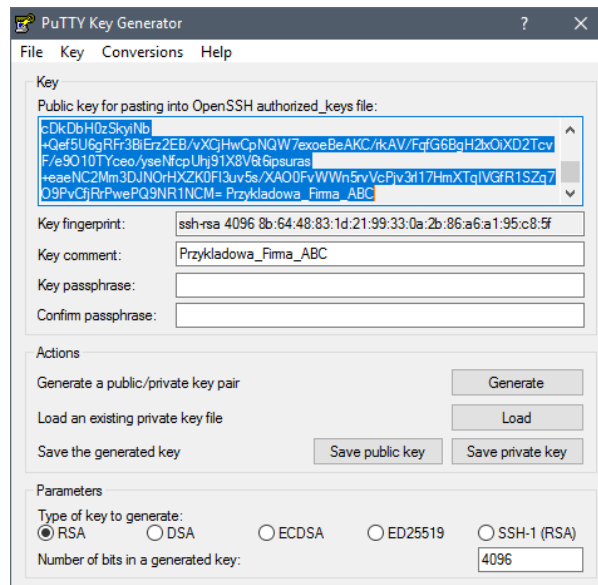
3. Zaznaczamy typ klucza RSA i ustawiamy jego długość na 4096 (jak na załączonym obrazku), bądź wybieramy klucz ED25519. Następnie klikamy na przycisk *Generate*:



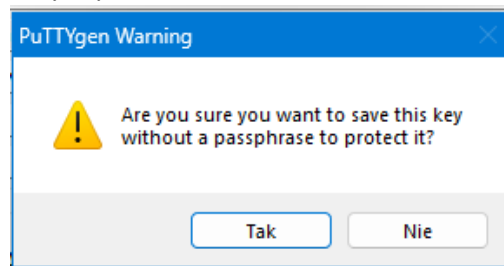
4. W trakcie generowania klucza poruszamy myszą nad oknem programu (zgodnie z komunikatem w aplikacji):



5. Po chwili klucz jest wygenerowany. Należy uzupełnić pole z komentarzem *Key comment*, umieszczając w nim np. nazwę firmy:

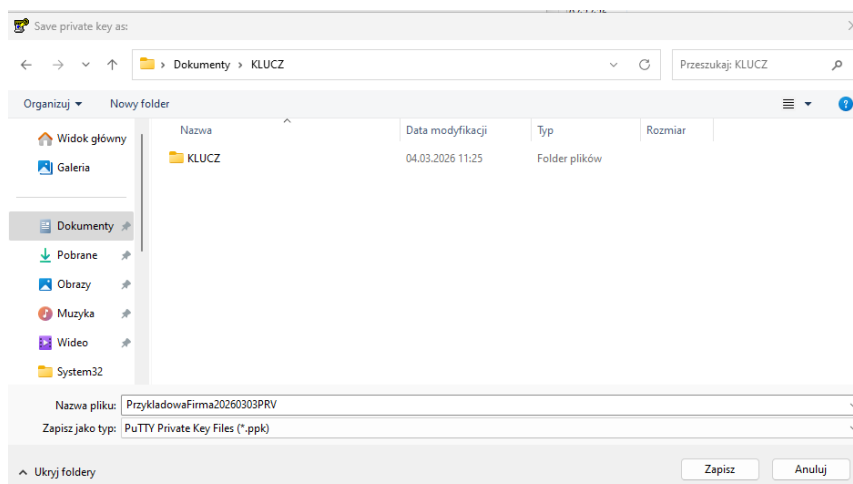


6. Następnie zapisujemy plik z kluczem prywatnym klikając na przycisk *Save private key*. Potwierdzamy, że chcemy zapisać klucz

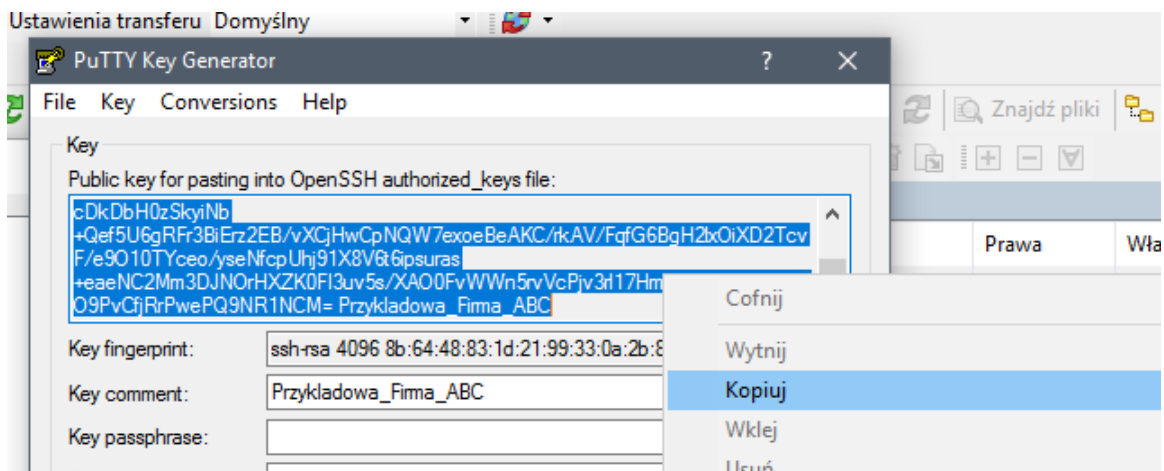


Uwaga! Należy zadbać o to, by miejsce jego zapisu nie było ogólnodostępne, jak pulpit, i plik nie dostał się w nieuprawnione ręce. Rekomendujemy utworzenie folderu o nazwie KLUCZ w Dokumentach

Plik dobrze jest nazwać w postaci – NazwaFirmyDataPRV bez spacji i polskich znaków. PRV oznacza klucz prywatny



7. Zawartość klucza publicznego kopiujemy w całości i zapisujemy do pliku tekstowego np. klucz.txt. Nie wysyłamy klucza wklejonego bezpośrednio w wiadomość email. Zapisany plik tekstowy wysyłamy na adres e-mail dostep.sftp@psgaz.pl



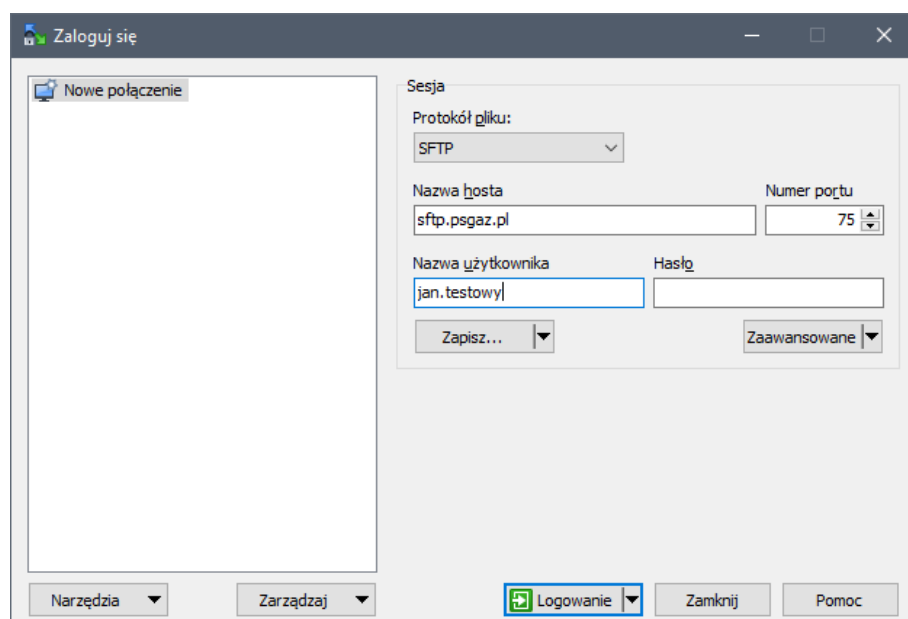
Uwaga! Klucz rozpoczyna się od frazy *ssh-rsa* (dla kluczy RSA) lub *ssh-ed25519* (dla kluczy ED25519), a kończy na naszym komentarzu z punktu 5 (którym może być np. nazwa firmy).

8. Oczekujemy na zwrotne potwierdzenie konfiguracji konta. Po otrzymaniu takiej informacji przechodzimy do konfiguracji połączenia.

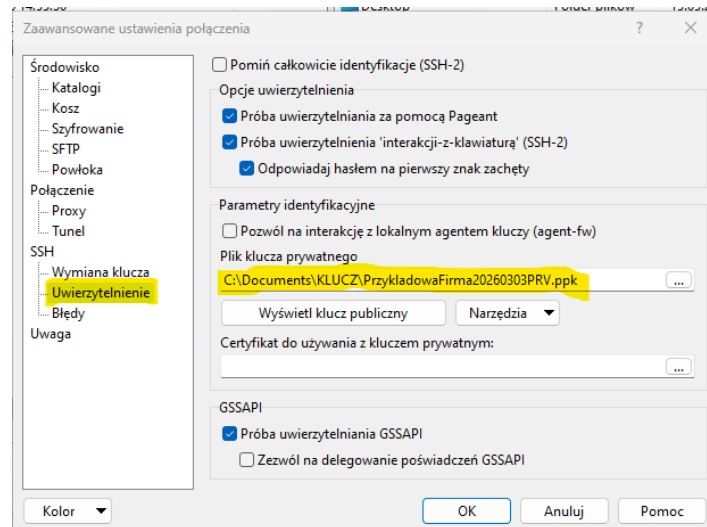
Konfiguracja połączenia do SFTP

1. Uruchamiamy klienta WinSCP i uzupełniamy pola:
 - 1.1. Protokół pliku – **SFTP**
 - 1.2. Nazwa hosta – **sftp.psgaz.pl**
 - 1.3. Numer portu – **75**
 - 1.4. Nazwa użytkownika – zgodnie z informacją otrzymaną od PSG.

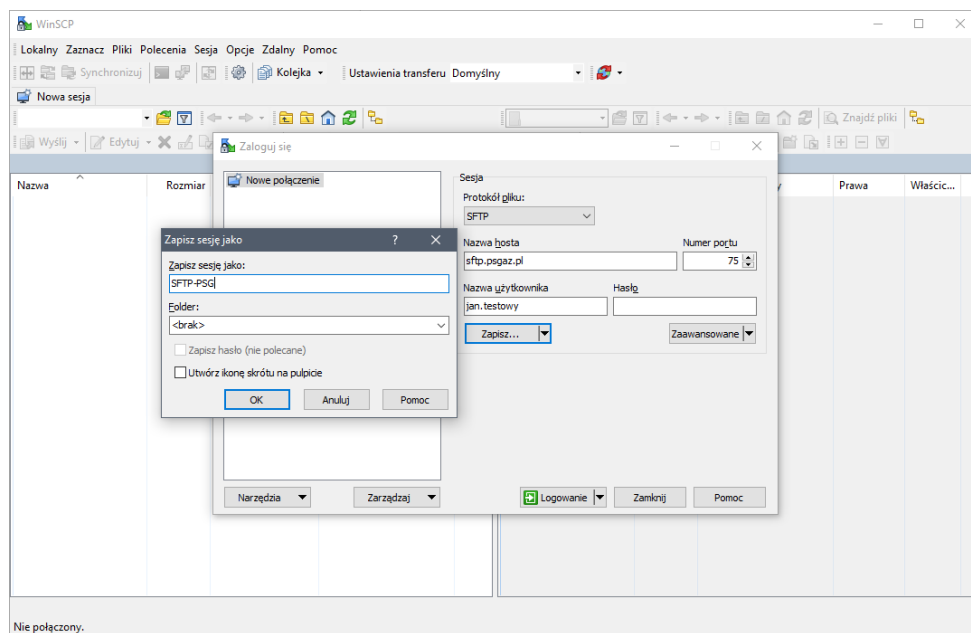
Następnie klikamy w przycisk *Zaawansowane*



2. W menu po lewej stronie wybieramy SSH -> Uwierzytelnienie. W polu Plik klucza prywatnego, wskazujemy położenie naszego pliku z kluczem prywatnym:

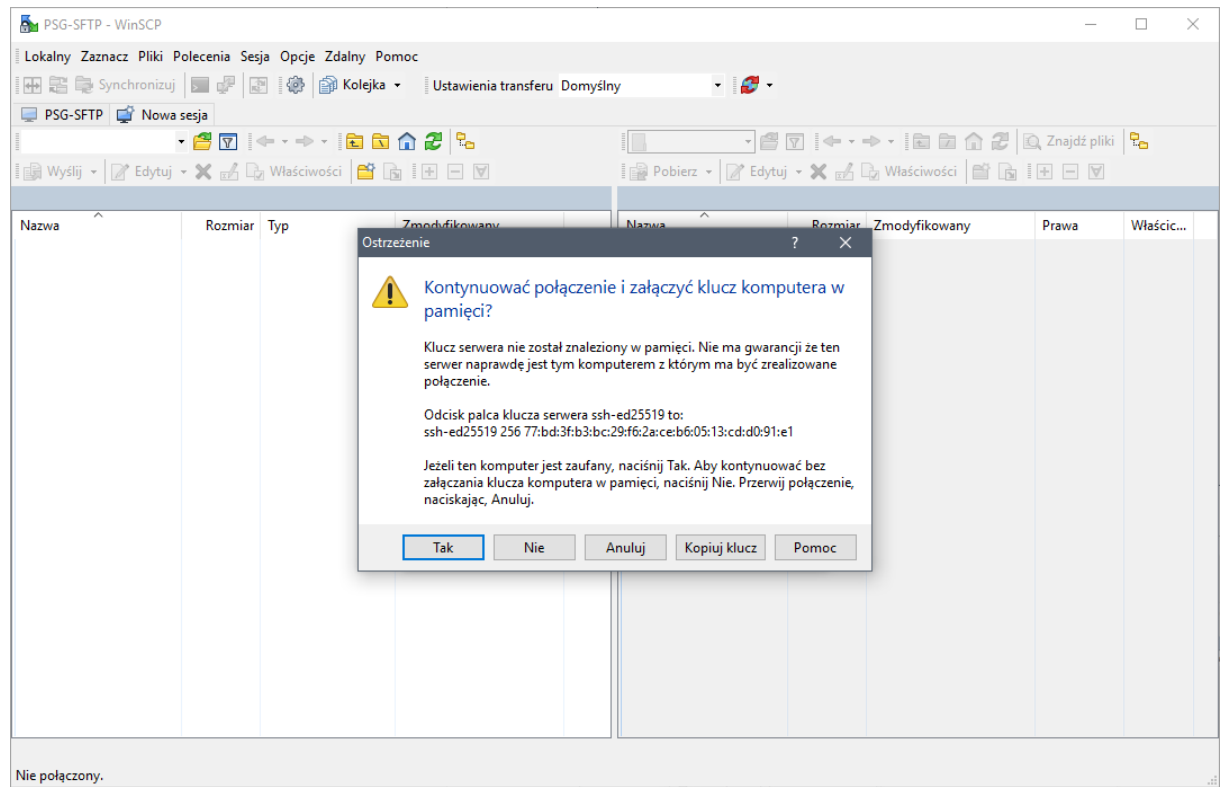


3. Zatwierdzamy ustawienia przyciskiem OK a następnie klikamy Zapisz..., by zapisać konfigurację naszego połączenia SFTP. Jako nazwę można podać np. SFTP-PSG:



Nawiązywanie bezpiecznego połączenia

By nawiązać połączenie, klikamy na uprzednio zdefiniowanej nazwie połączenia. W oknie z zapytaniem odpowiadamy twierdząco:



4. Po chwili mamy nawiązane bezpieczne, szyfrowane połączenie:

