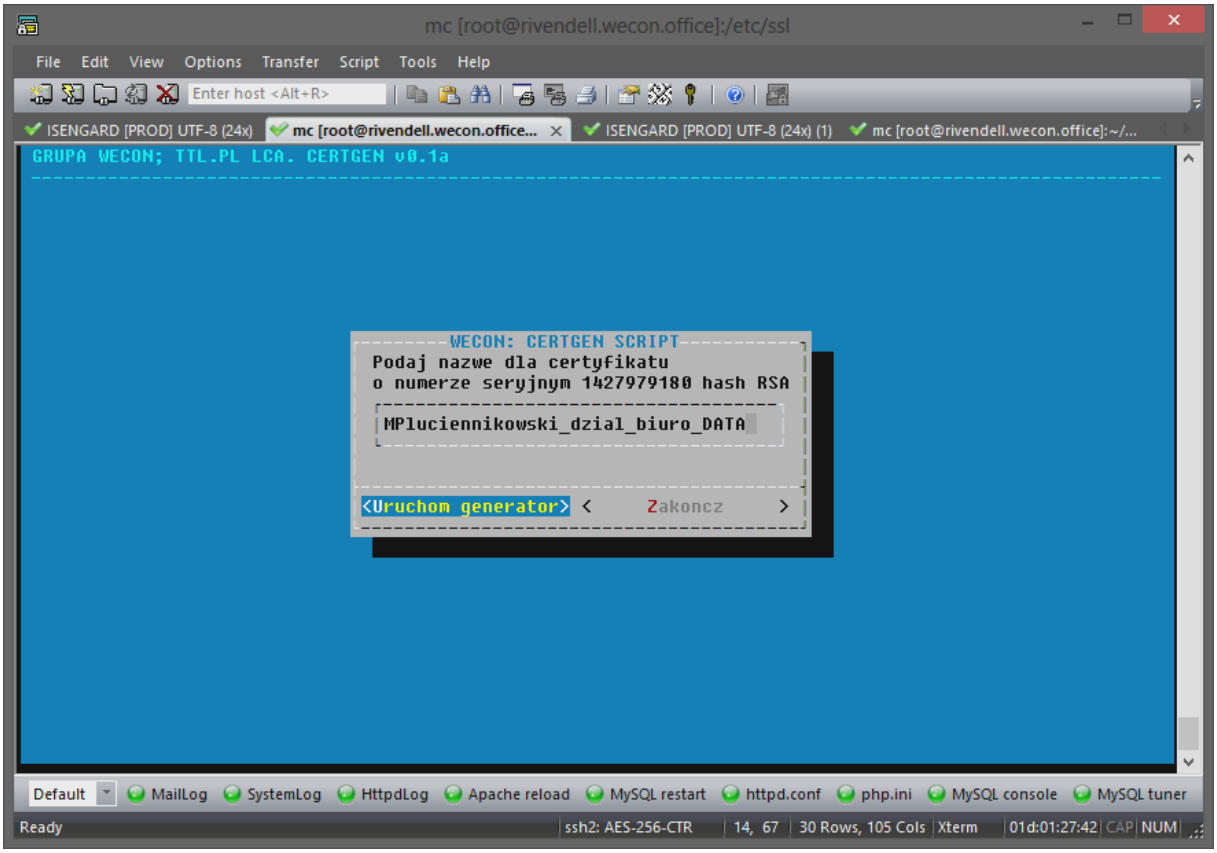
Generowanie certyfikatu dla aplikacji klienckiej BackOffice SRF.

Uruchomienie generatora następuje automatycznie po zalogowaniu się na konto certgen w systemie rivendell. Haseł w tej instrukcji naturalnie podawać nie będę :)

Adresy hostów to (w sieci lokalnej):

rivendell.wecon.office

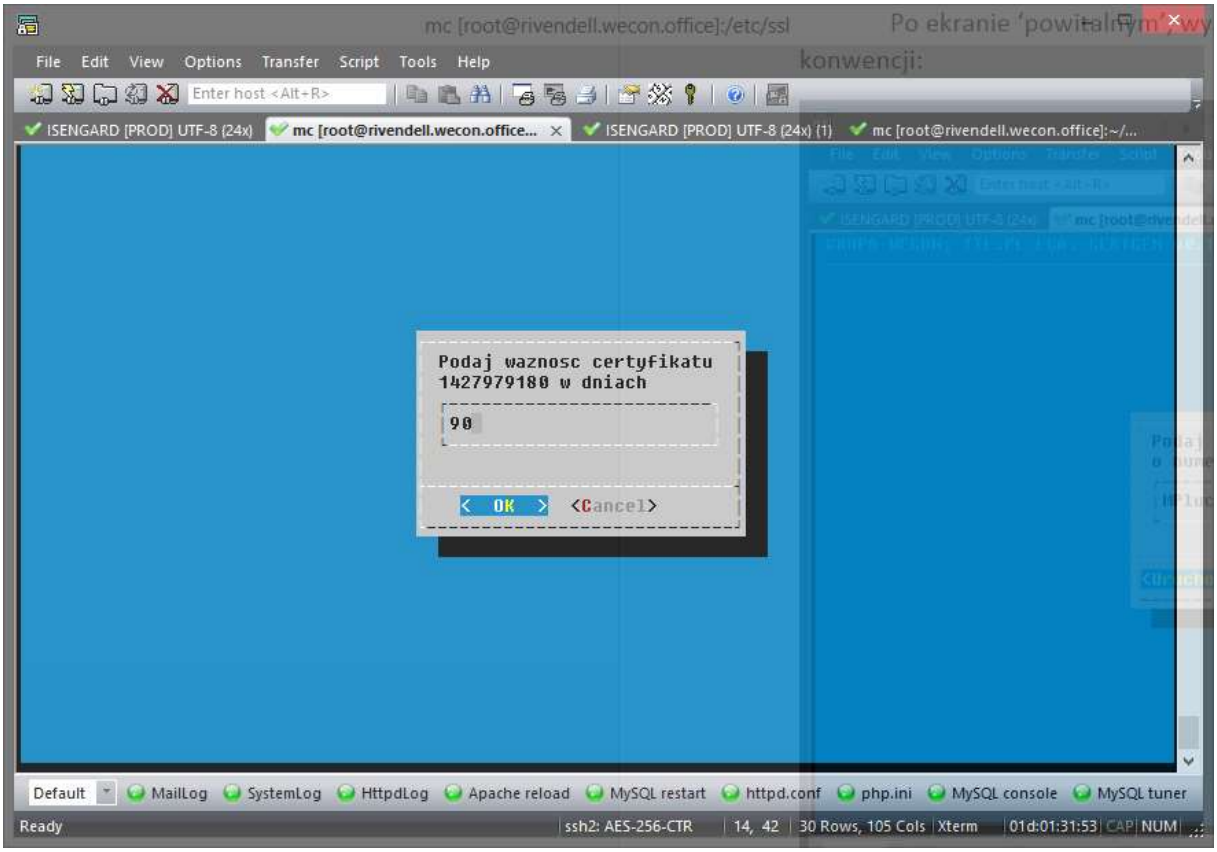
Po ekranie ‘powitalnym’, wyskoczy ekran z monitem o nazwę certyfikatu. Trzymamy się konwencji:



PierwszaLiteraImienia + Nazwisko + nazwa działu + numer oddziału firmy + data w formacie YYYYMMDD

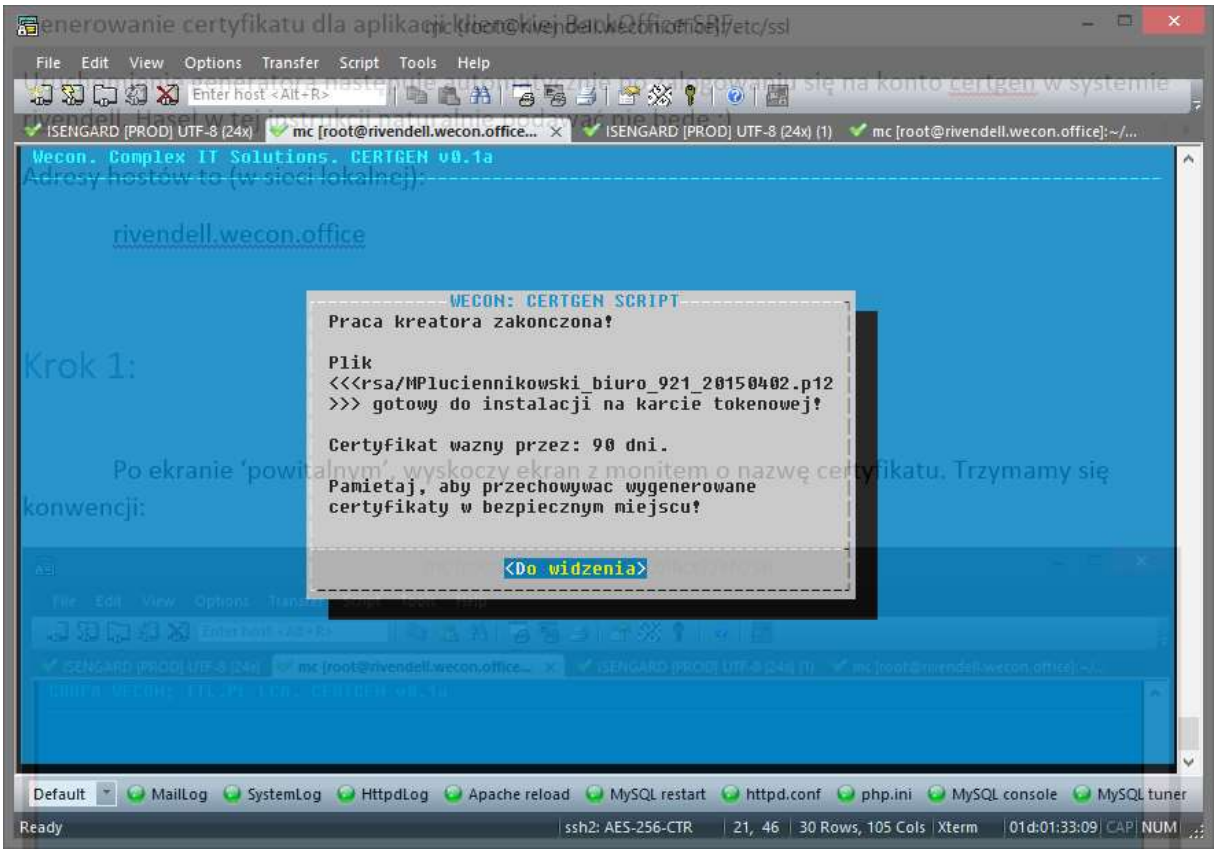
Klikamy ‘Uruchom generator’.

Podajemy ważność certyfikatu. Dla biura i managerów jest to maksymalny okres 90 dni. Tak zarządziła dyrekcja.

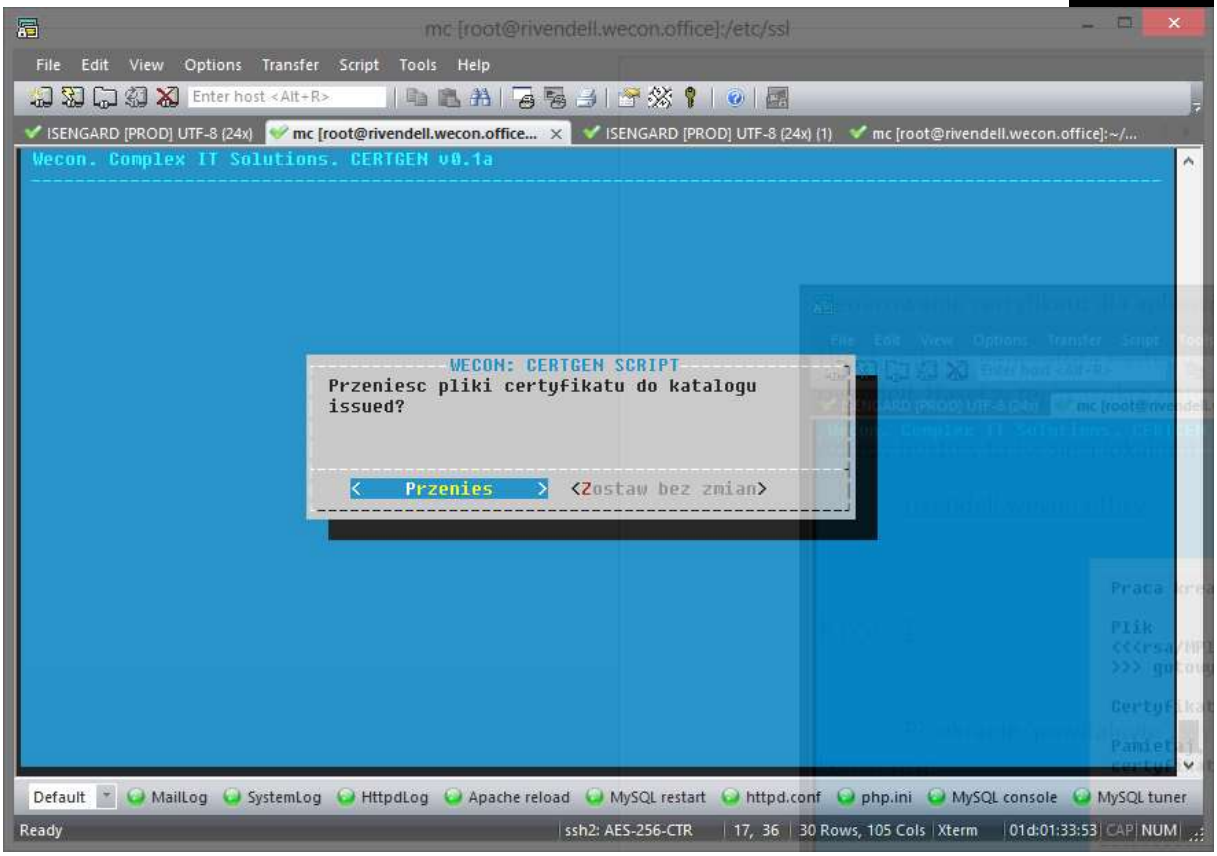


Klikamy ‘OK’.

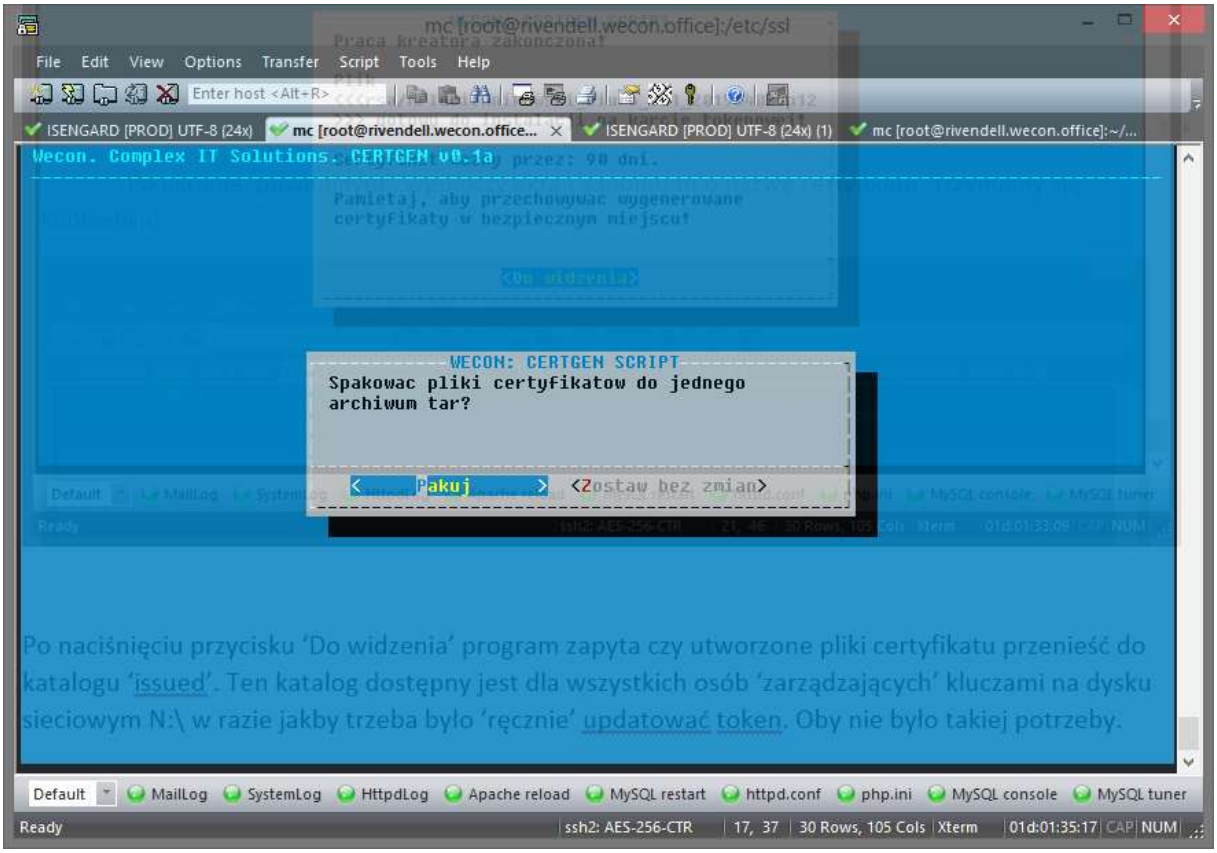
Na ekranie wyświetli się sporo śmieci, a po wszystkim program wyrzuci podziękowanie. Nie jest to koniec i trzeba nacisnąć mylący przycisk ‘Do widzenia’.



Po naciśnięciu przycisku ‘Do widzenia’ program zapyta czy utworzone pliki certyfikatu przenieść do katalogu ‘issued’. Ten katalog dostępny jest dla wszystkich osób ‘zarządzających’ kluczami na dysku sieciowym N:\ w razie jakby trzeba było ‘ręcznie’ updatować token. Oby nie było takiej potrzeby.

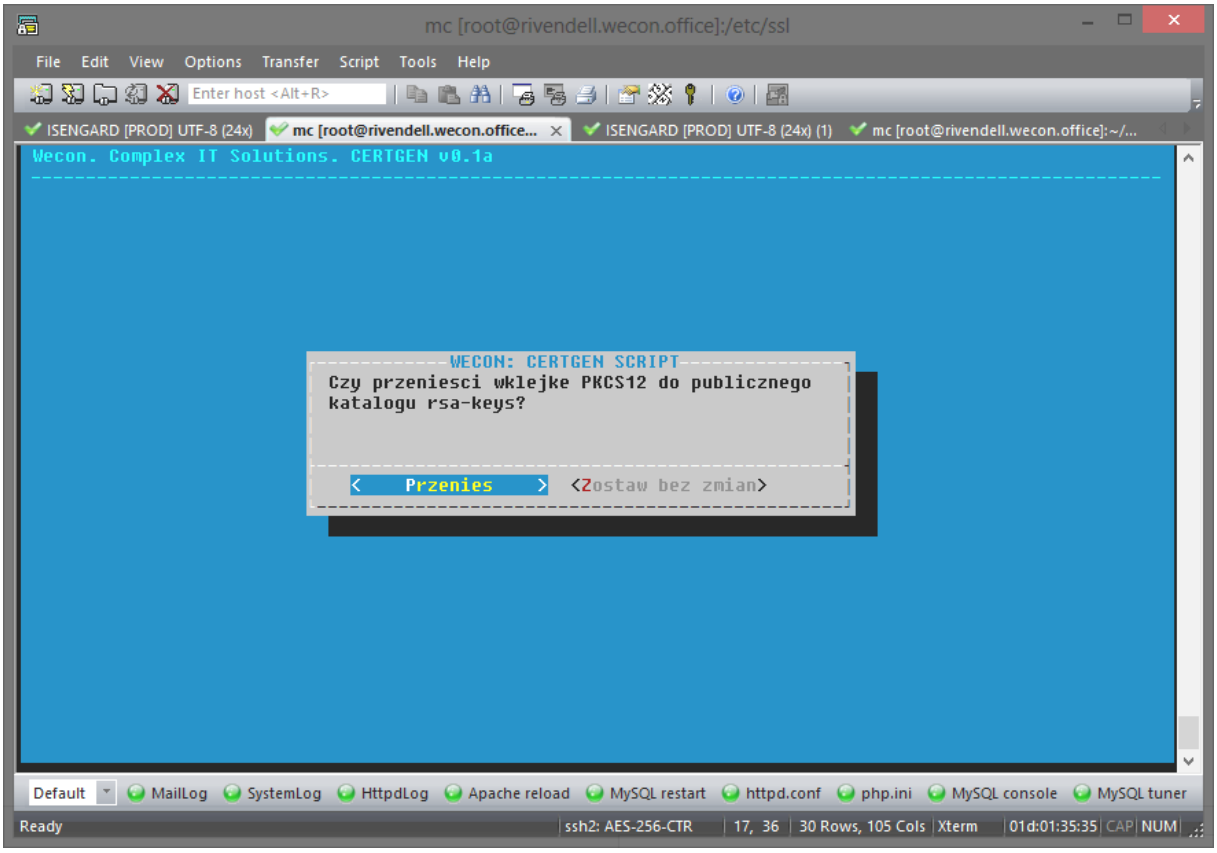


Naciskamy przycisk ‘Przenieś’ i potwierdzamy pakowanie plików certyfikatu do jednego tarballa.

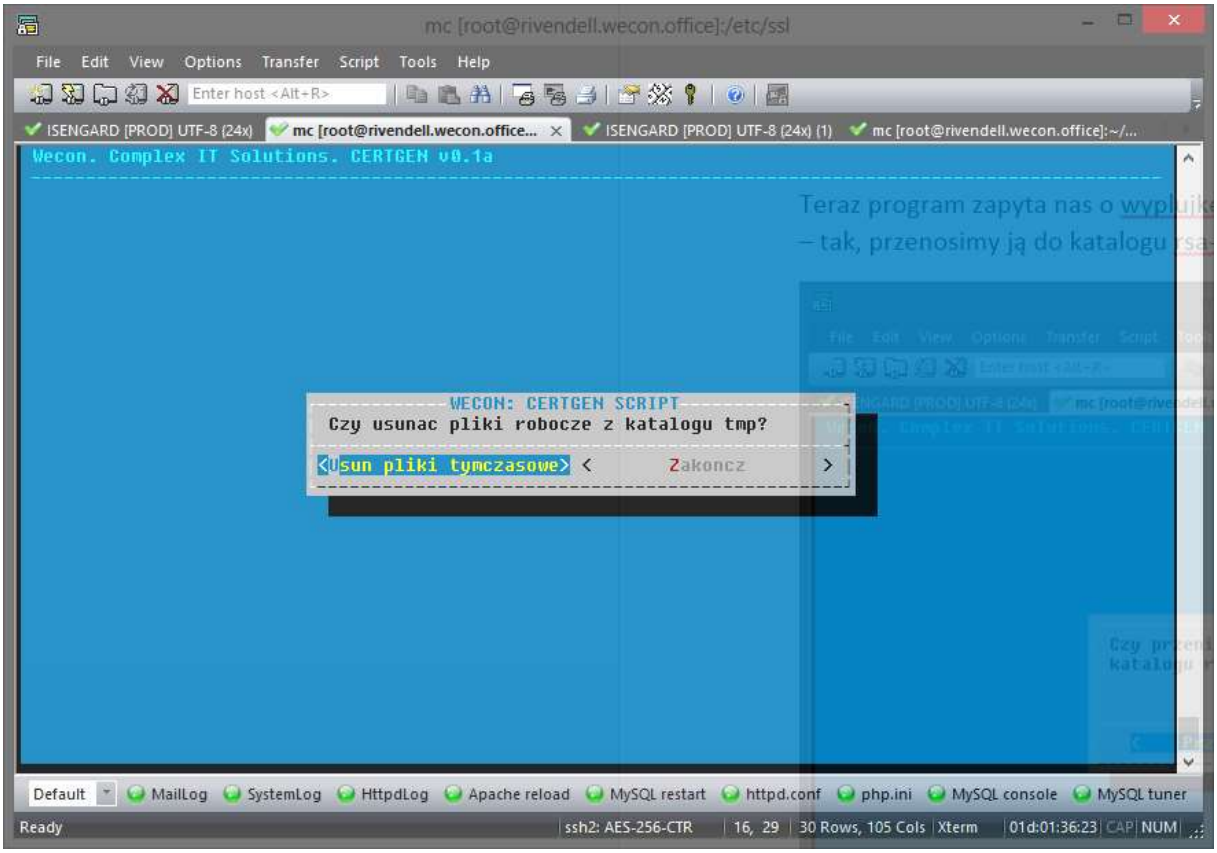


Po naciśnięciu przycisku ‘Do widzenia’ program zapyta czy utworzone pliki certyfikatu przenieść do katalogu ‘issued’. Ten katalog dostępny jest dla wszystkich osób ‘zarządzających’ kluczami na dysku sieciowym N:\ w razie jakby trzeba było ‘ręcznie’ updatować token. Oby nie było takiej potrzeby.

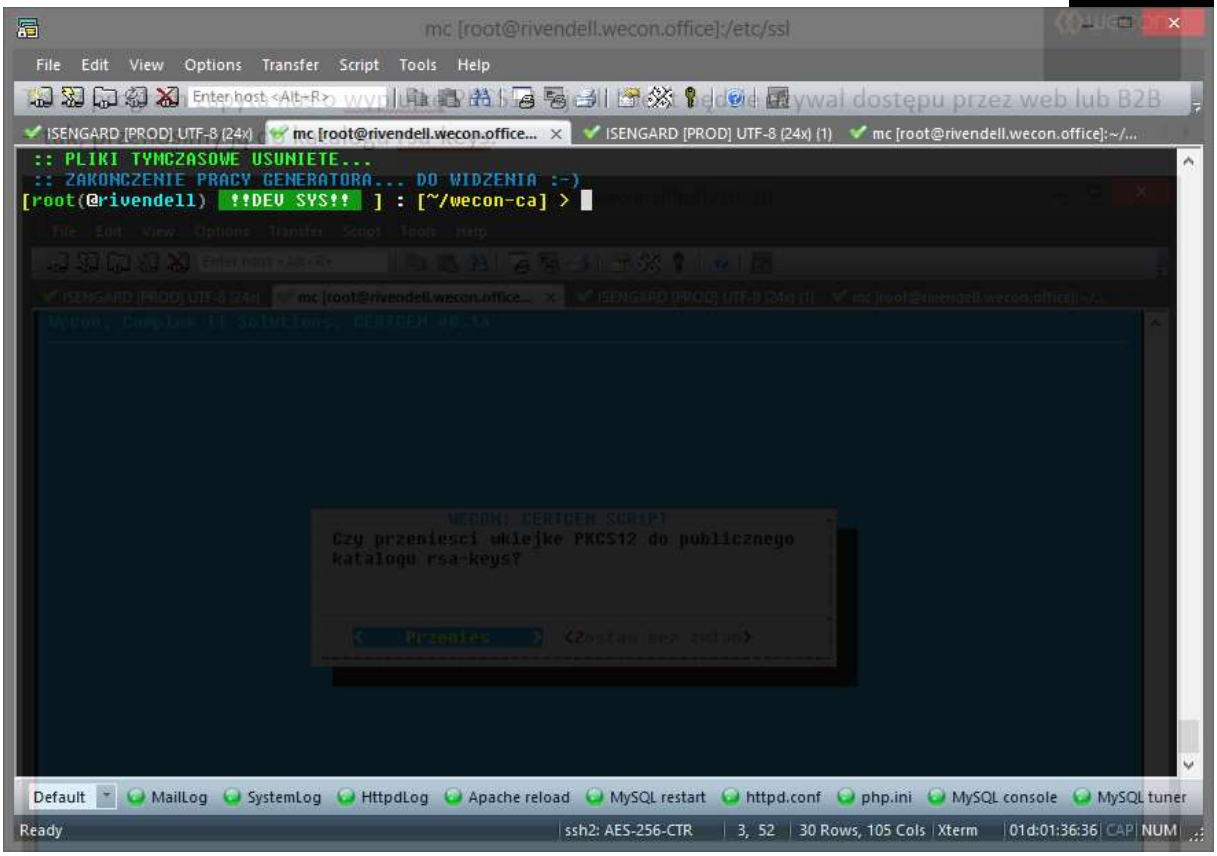
Teraz program zapyta nas o wyplujkę PKCS12 – jeśli klient będzie używał dostępu przez web lub B2B – tak, przenosimy ją do katalogu rsa-keys.



Czyścimy tempa:



I tyle. Pamiętać należy, że w tym momencie karta powinna być włożona do czytnika. Program przerzuci wygenerowane certyfikaty, a pliki, które zostaną na dysku serwera zabezpieczy maską, aby tylko root mógł je odczytywać.

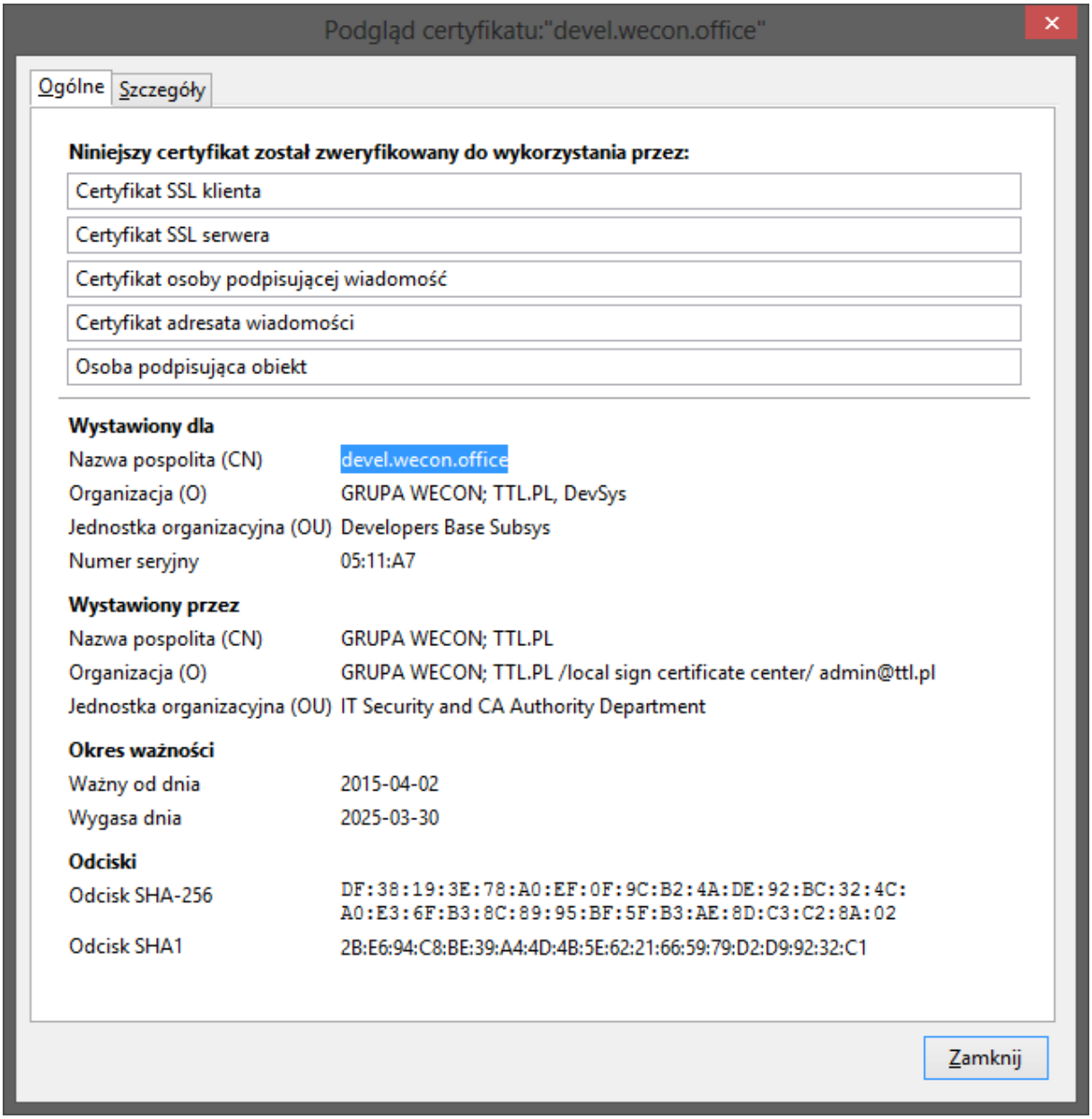


Kartę można oddać Klientowi.

Kilka uwag:

1. W nowej wersji systemu BackOffice ważność karty sprawdzana jest co kilka minut. Tydzień przed utratą ważności Klientowi wyskakuje monit o przedłużenie certyfikatu. Wygląda to mniej więcej tak:

2. Jeśli Klient jest ‘odrzucany’, sprawdzić wyplujkę po stronie jakiejkolwiek przeglądarki po próbie zalogowania przez web B2B:



Tylko w/w klucz będzie działał z najnowszą wersją serwera autentykacji i logowania. Jeśli taki klucz nie zgłosił się, trzeba go ‘doinstalować ręcznie’ chociażby z tokena /każdy token ma wgrany fabrycznie nasz klucz CA/.

W razie czego, pytać/dzwonić/mailować:

Michał Płuciennikowski, GSM 535 755 555.