



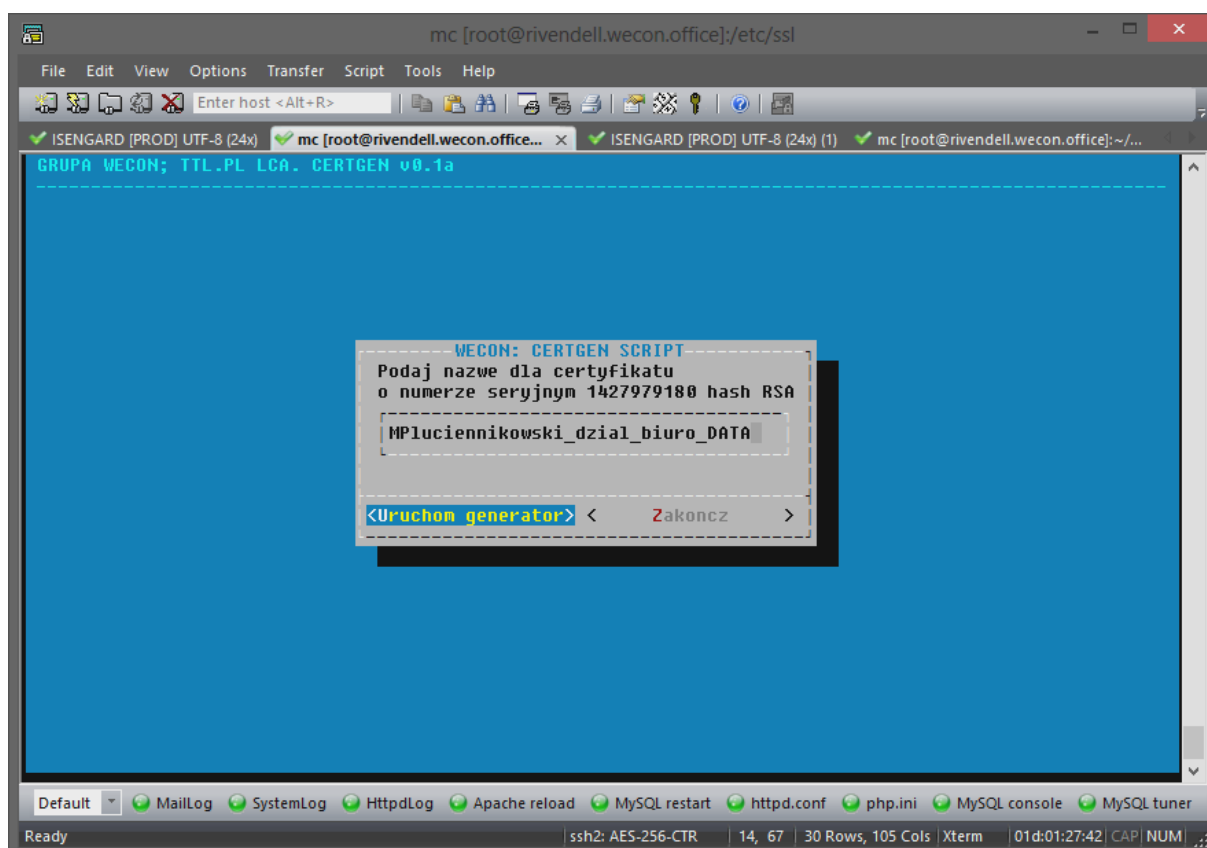
Generowanie certyfikatu dla aplikacji klienckiej BackOffice SRF.

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:

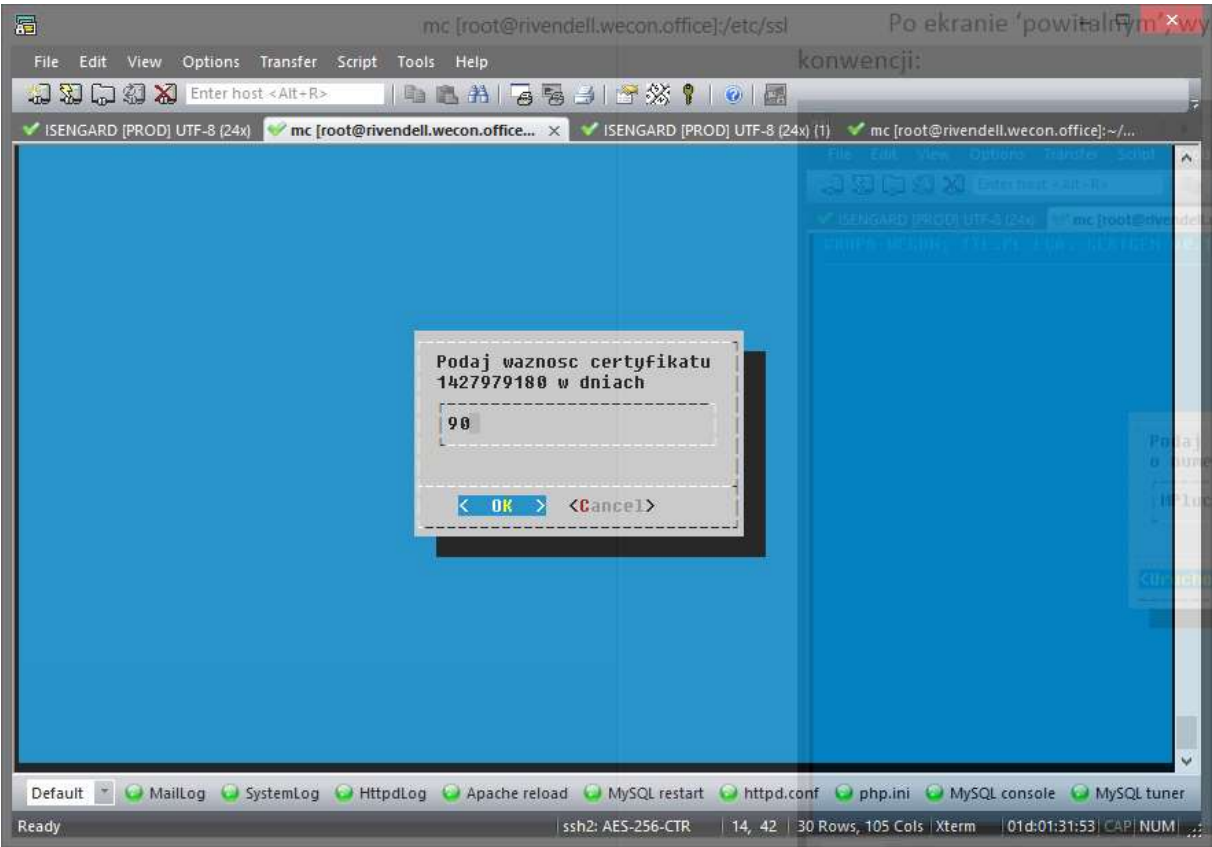


PierwszaLiteraImienia + Nazwisko + nazwa działu + numer oddziału firmy + data w formacie YYYYMMDD

Klikamy 'Uruchom generator'.



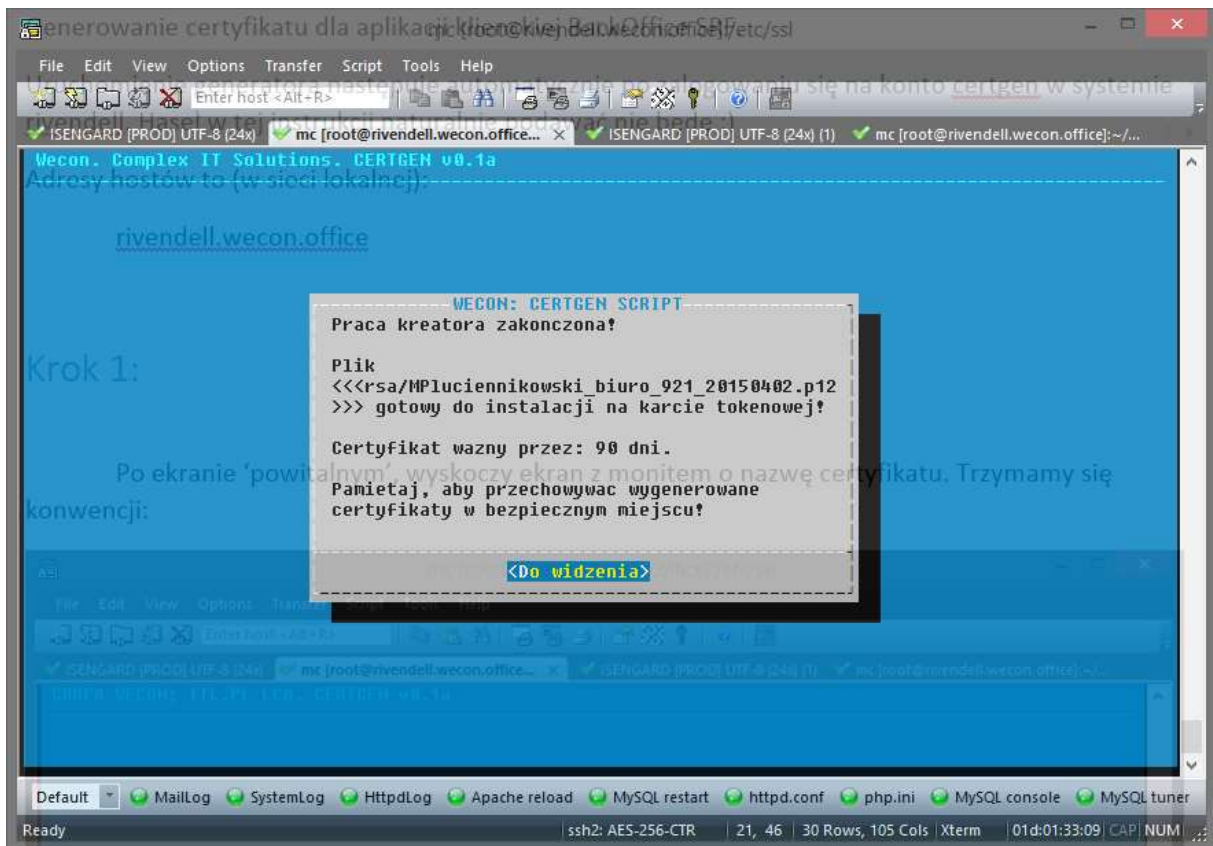
Podajemy ważność certyfikatu. Dla biura i managerów jest to maksymalny okres 90 dni. Tak zarządziła dyrekcja.



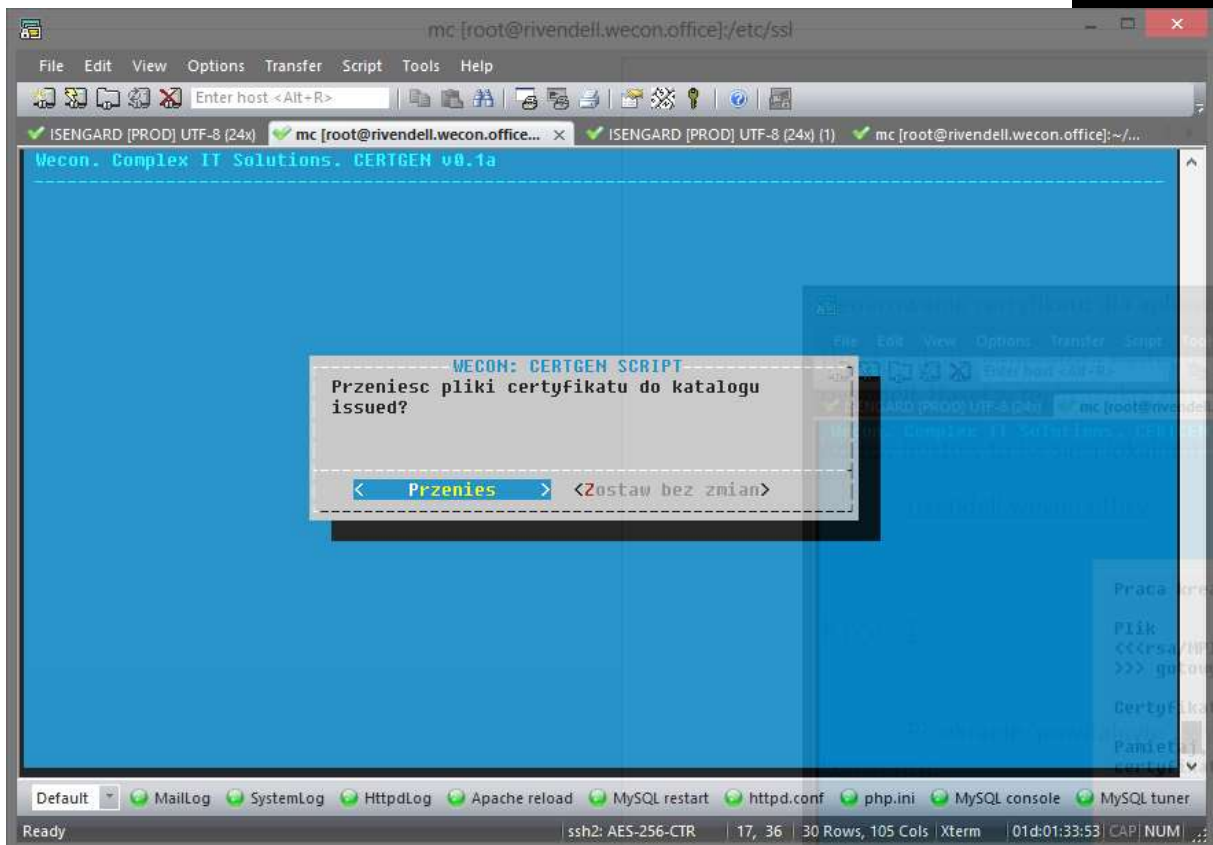
Klikamy 'OK'.



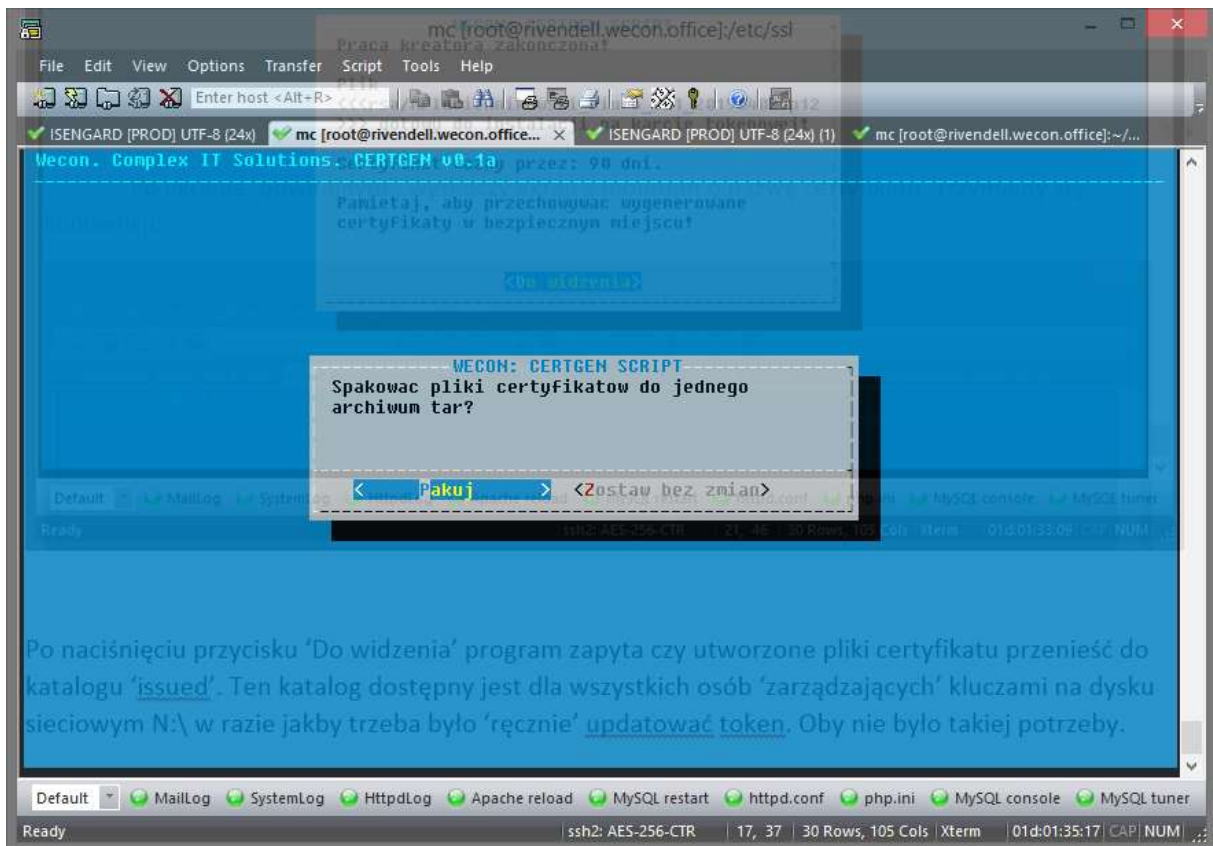
Na ekranie wyświetli się sporo śmieci, a po wszystkim program wyrzuci podziękowanie. Nie jest to koniec i trzeba nacisnąć mylący przycisk 'Do widzenia'.



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' aktualizować token. Oby nie było takiej potrzeby.

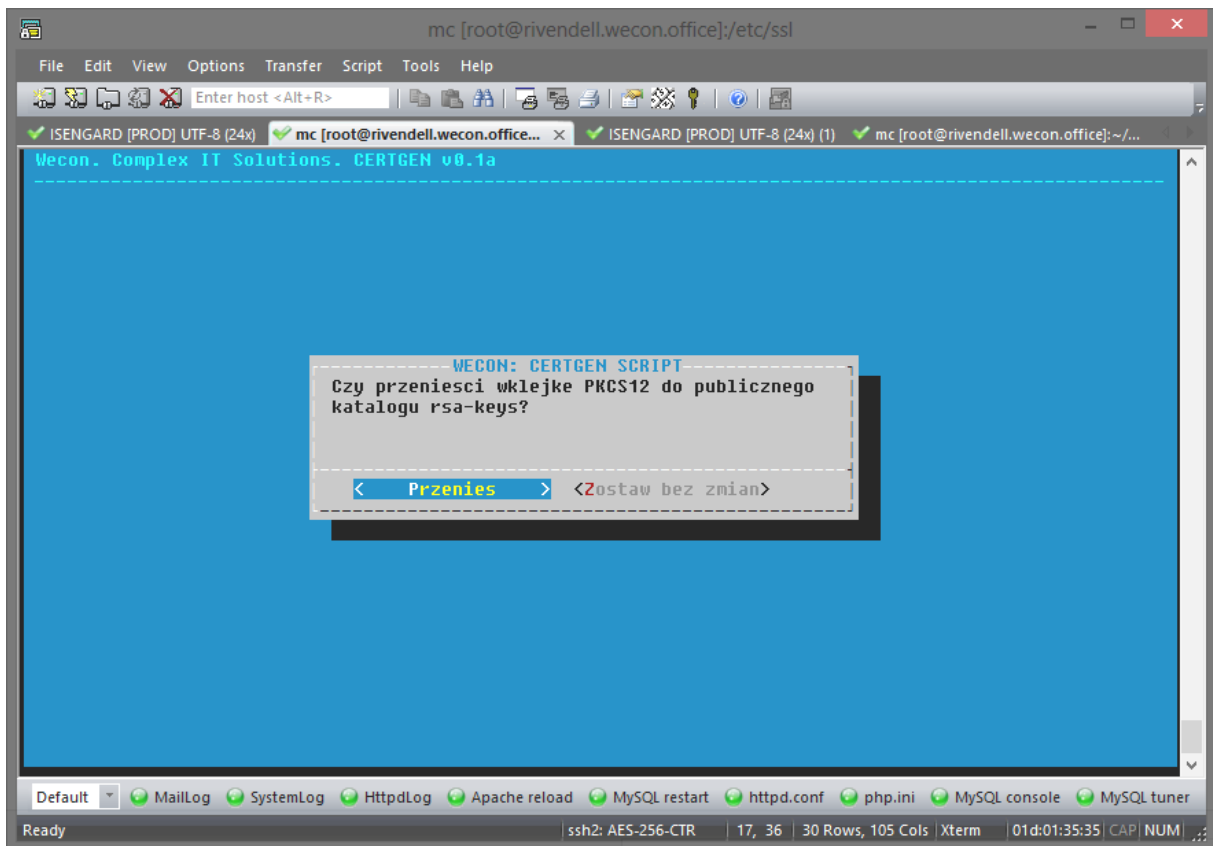


Naciskamy przycisk 'Przenies' i potwierdzamy pakowanie plików certyfikatu do jednego tarballa.



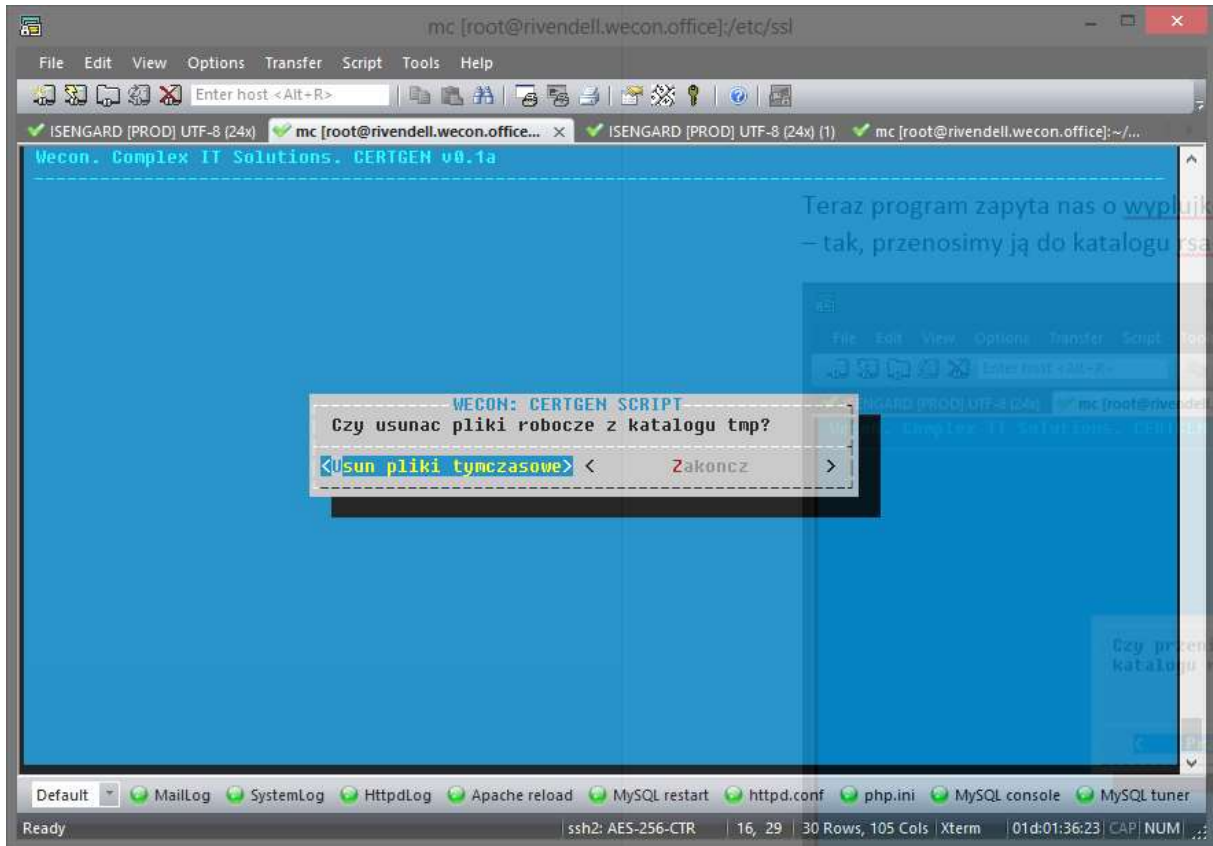


Teraz program zapyta nas o wyplukę PKCS12 – jeśli klient będzie używał dostępu przez web lub B2B – tak, przenosimy ją do katalogu rsa-keys.

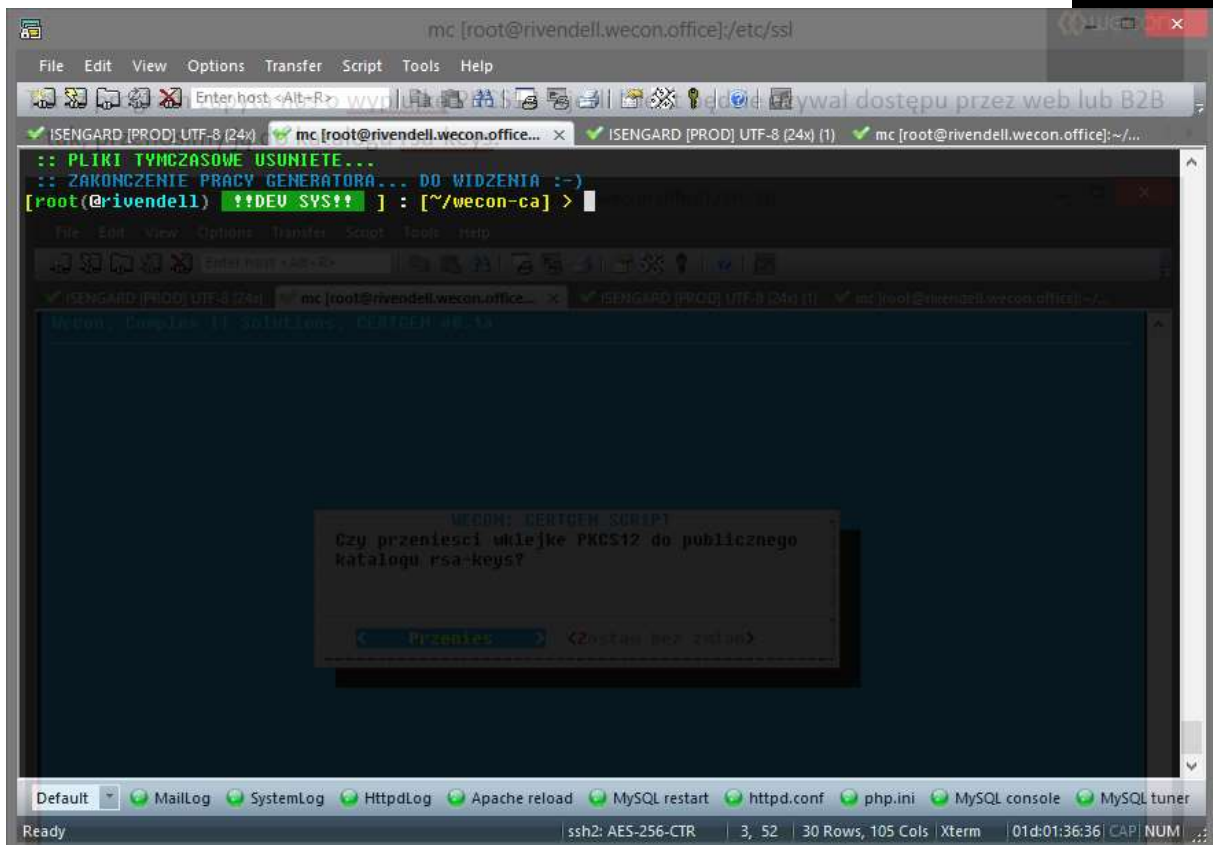




Czyścimy tempa:



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



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 'odrzucony', sprawdzić wyplukę po stronie jakiegokolwiek przeglądarki po próbie zalogowania przez web B2B:

Podgląd certyfikatu:"devel.wecon.office"

Ogólne Szczegóły

Niniejszy certyfikat został zweryfikowany do wykorzystania przez:

Certyfikat SSL klienta
Certyfikat SSL serwera
Certyfikat osoby podpisującej wiadomość
Certyfikat adresata wiadomości
Osoba podpisująca obiekt

Wystawiony dla

Nazwa pospolita (CN)	devel.wecon.office
Organizacja (O)	GRUPA WECON; TTL.PL, DevSys
Jednostka organizacyjna (OU)	Developers Base Subsys
Numer seryjny	05:11:A7

Wystawiony przez

Nazwa pospolita (CN)	GRUPA WECON; TTL.PL
Organizacja (O)	GRUPA WECON; TTL.PL /local sign certificate center/ admin@ttl.pl
Jednostka organizacyjna (OU)	IT Security and CA Authority Department

Okres ważności

Ważny od dnia	2015-04-02
Wygasa dnia	2025-03-30

Odciski

Odcisk SHA-256	DF:38:19:3E:78:A0:EF:0F:9C:B2:4A:DE:92:BC:32:4C:A0:E3:6F:B3:8C:89:95:BF:5F:B3:AE:8D:C3:C2:8A:02
Odcisk SHA1	2B:E6:94:C8:BE:39:A4:4D:4B:5E:62:21:66:59:79:D2:D9:92:32:C1

Zamknij

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.