

Zadania do samodzielnej realizacji w domu (Moduł 4)

Zadanie 1

Jesteś administratorem systemów w firmie X.

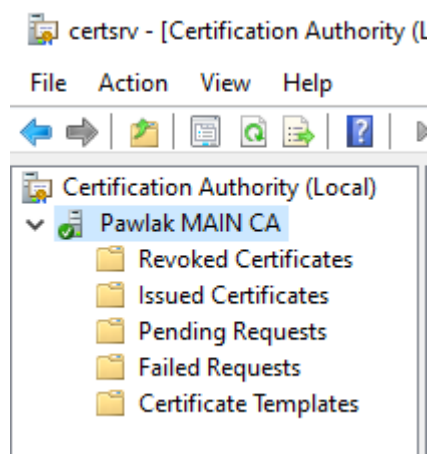
W organizacji zapadła decyzja, aby wdrożyć lokalną infrastrukturę klucza publicznego zintegrowaną z usługą Active Directory, na kontrolerze domeny Windows Server "London".

Twoim zadaniem jest więc zainstalowanie głównego serwera certyfikującego zintegrowanego z usługą Active Directory w systemie Windows Server "London", dla którego należy określić nazwę "{Nazwisko} MAIN CA" (gdzie pod {Nazwisko} należy podstawić własne nazwisko - jest to warunkiem zaliczenia sprawozdania, przykładowo: Kowalski MAIN CA), instalując rolę "Usługi certyfikatów Active Directory" wraz z usługami roli: "Urząd certyfikacji" oraz "Rejestracja w sieci Web dla urzędu certyfikacji".

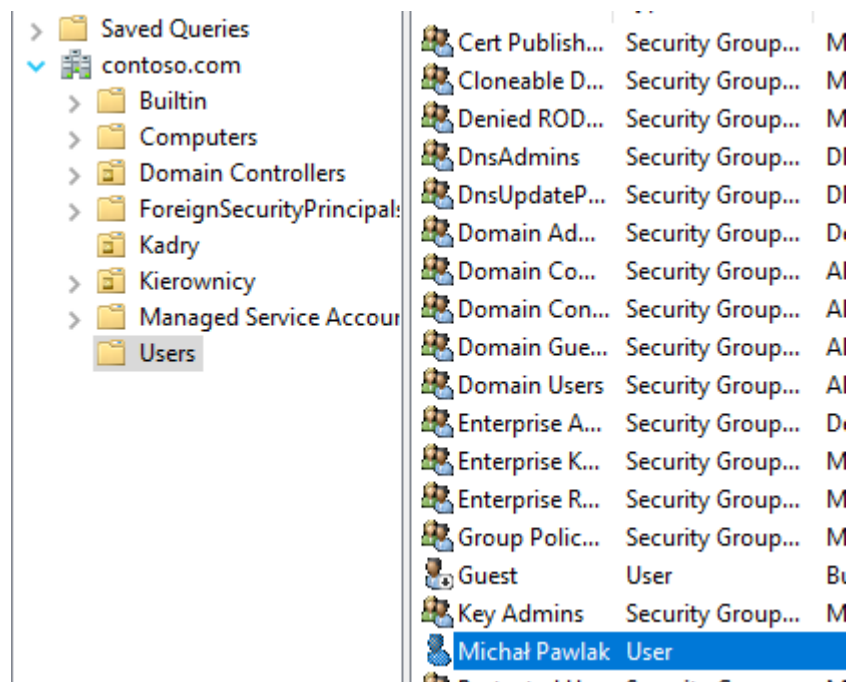
Ponadto otrzymałeś również zamieszczoną poniżej listę zadań, które powinieneś wdrożyć wykorzystując zainstalowany lokalny urząd certyfikujący:

1. Utworzyć w bazie Active Directory nowego użytkownika "*Imię Nazwisko*" (gdzie pod {Imię Nazwisko} należy podstawić własne imię i nazwisko - jest to warunkiem zaliczenia sprawozdania, przykładowo: *Jan Kowalski*), a następnie zalogować się na niego w systemie Windows 8/10 i przetestować możliwość zaszyfrowania przez tego użytkownika pliku "C:\test\{nazwisko}.txt" (gdzie plik ten należy najpierw utworzyć, a pod {nazwisko} należy podstawić własne nazwisko - jest to warunkiem zaliczenia sprawozdania, przykładowo: *kowalski.txt*) z wykorzystaniem systemu EFS, w taki sposób aby został do tego celu użyty certyfikat podpisany przez lokalny urząd certyfikujący zintegrowany z Active Directory (co należy zweryfikować). Należy również zweryfikować brak możliwości odczytu tegoż pliku przez innego dowolnego użytkownika.
2. Przetestować także możliwość nadania przez użytkownika "*Imię Nazwisko*" dostępu do zaszyfrowanego pliku dla innych użytkowników na przykładzie użytkownika *Witold Sup*.

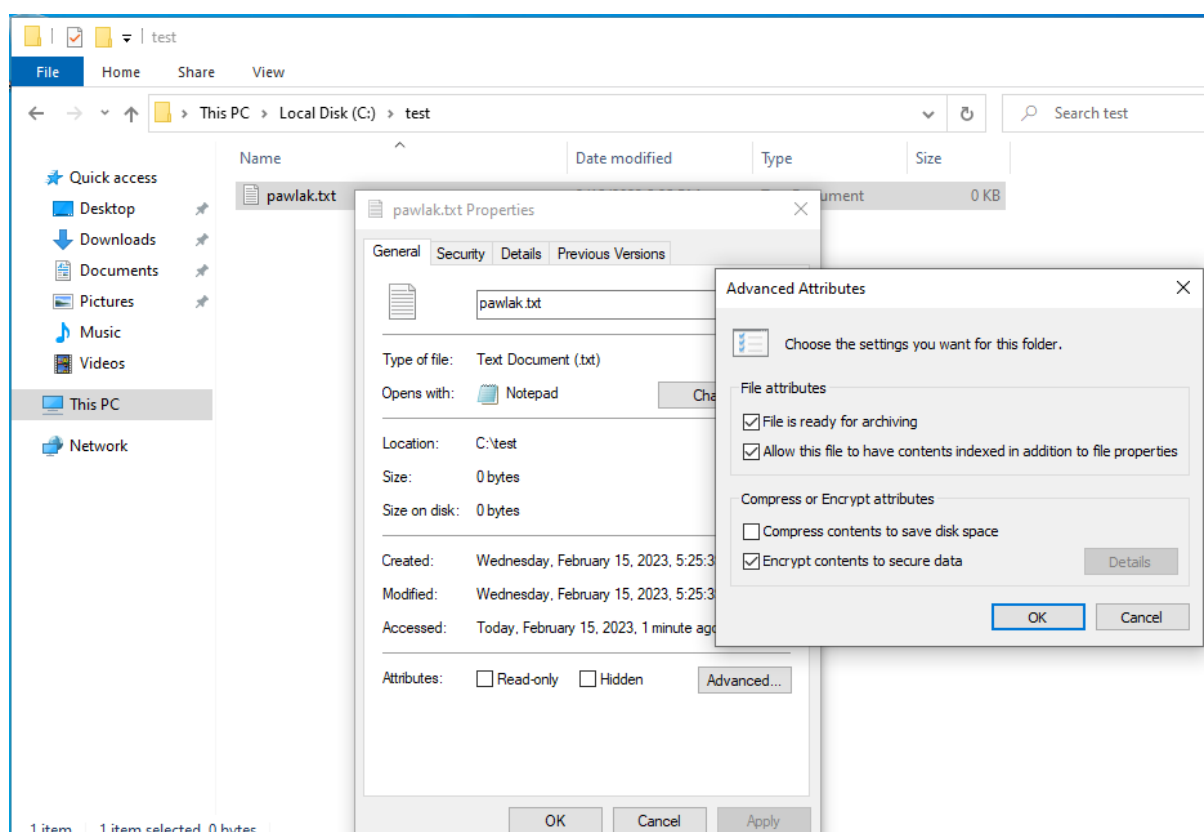
3. Pan *Jacek Gula* ma uzyskać "przymusowy" dostęp do wszystkich danych zaszyfrowanych w ramach systemu EFS na komputerach firmy, co należy wdrożyć, a następnie przetestować na przykładzie pliku "C:\test\{nazwisko}.txt".
-

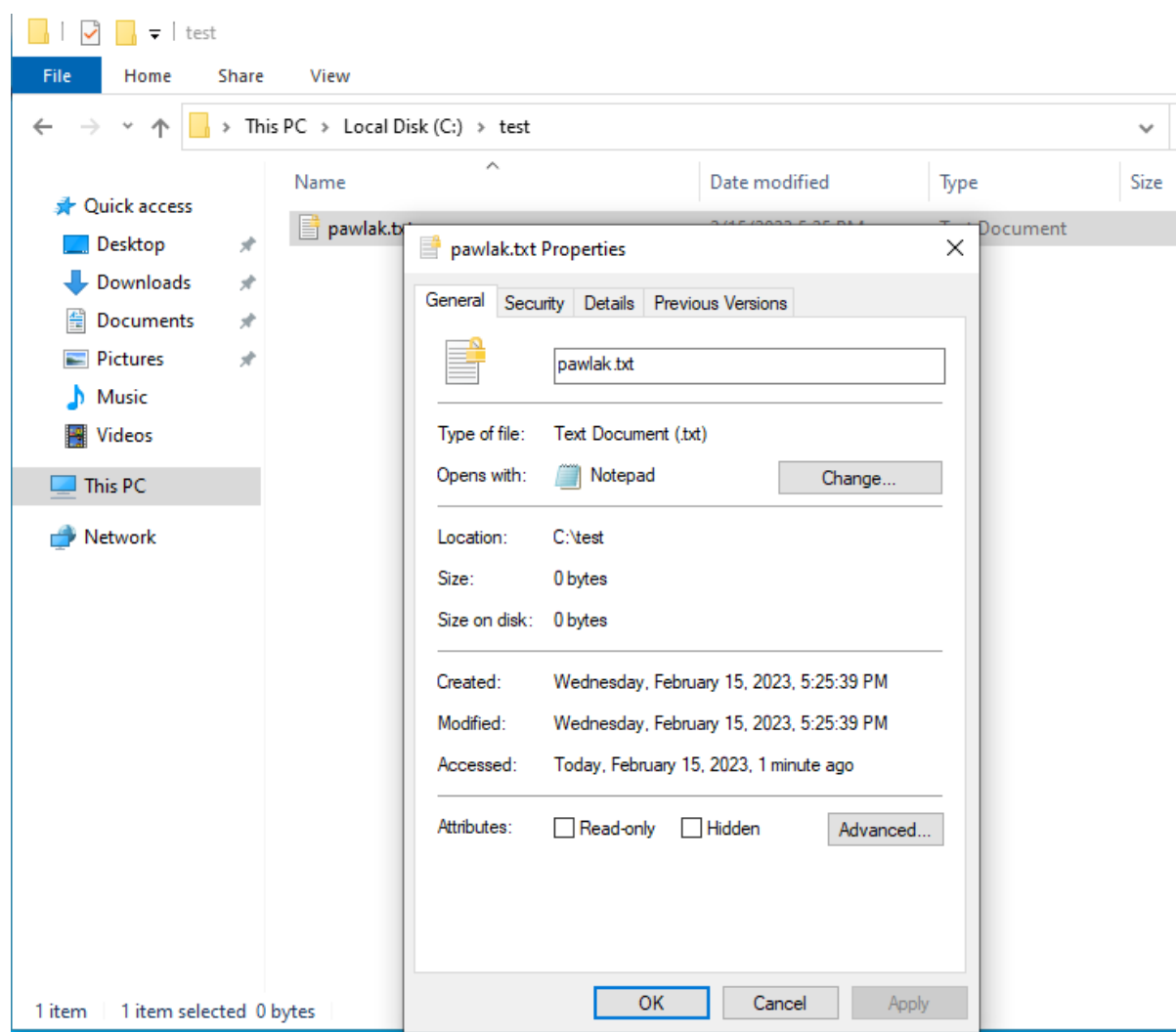
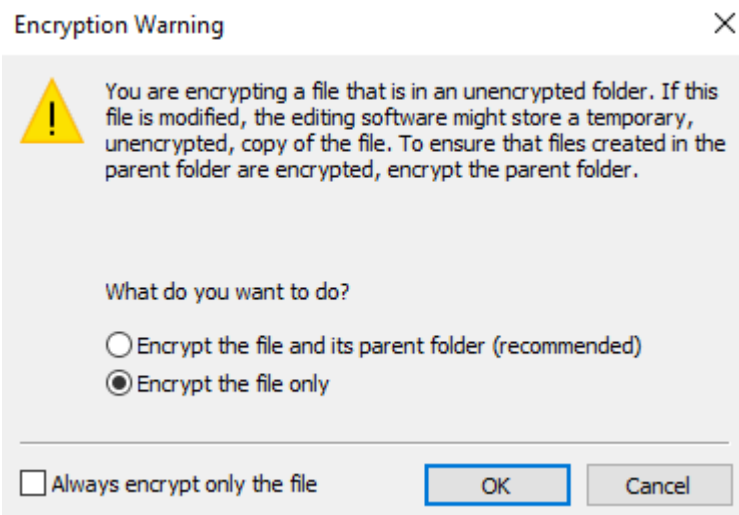


1. Utworzyć w bazie Active Directory nowego użytkownika "*Imię Nazwisko*" (gdzie pod {Imię Nazwisko} należy podstawić własne imię i nazwisko - jest to warunkiem zaliczenia sprawozdania, przykładowo: *Jan Kowalski*), a następnie zalogować się na niego w systemie Windows 8/10 i przetestować możliwość zaszyfrowania przez tego użytkownika pliku "C:\test\{nazwisko}.txt" (gdzie plik ten należy najpierw utworzyć, a pod {nazwisko} należy podstawić własne nazwisko - jest to warunkiem zaliczenia sprawozdania, przykładowo: *kowalski.txt*) z wykorzystaniem systemu EFS, w taki sposób aby został do tego celu użyty certyfikat podpisany przez lokalny urząd certyfikujący zintegrowany z Active Directory (co należy zweryfikować). Należy również zweryfikować brak możliwości odczytu tegoż pliku przez innego dowolnego użytkownika.

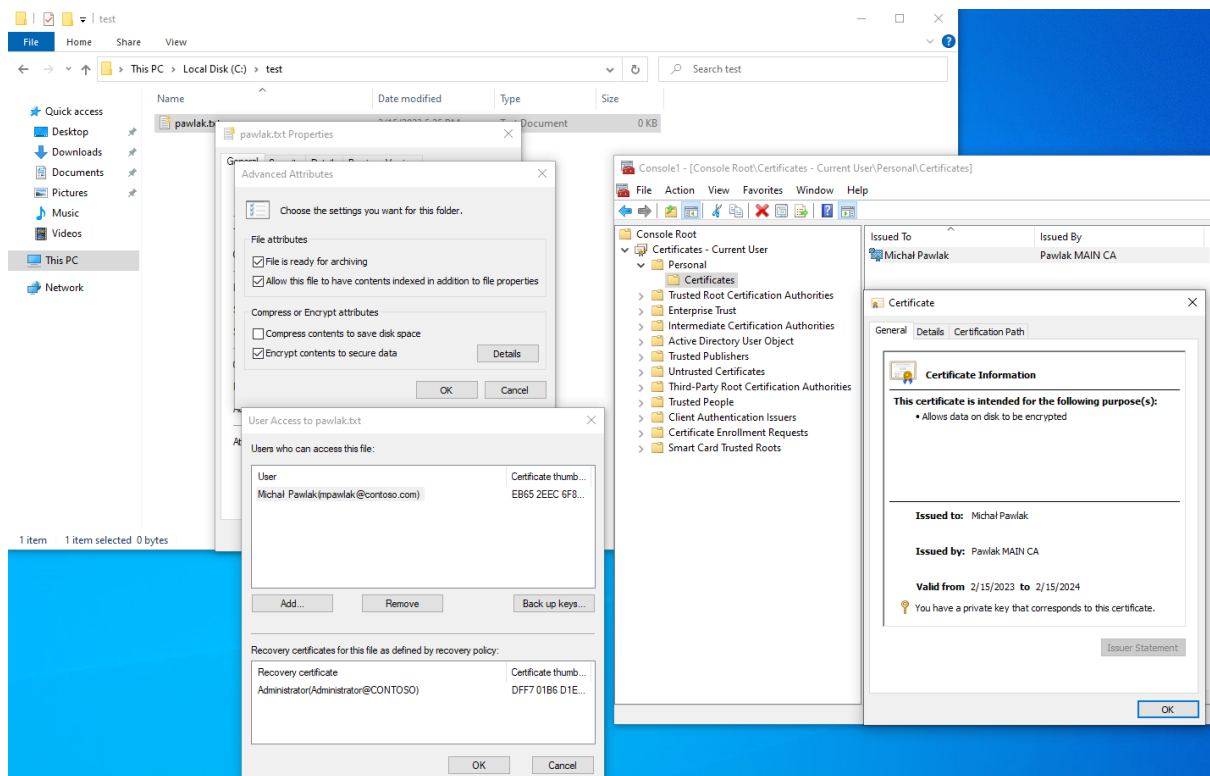


na windowsie "Nowak"



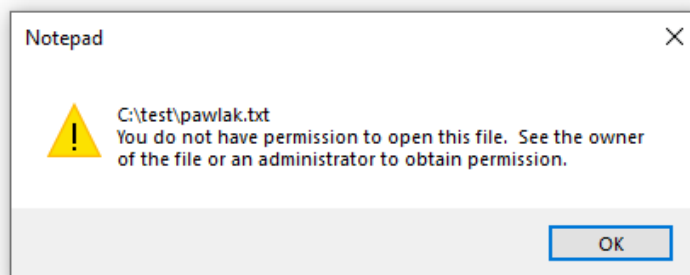
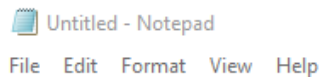


Plik został zaszyfrowany.



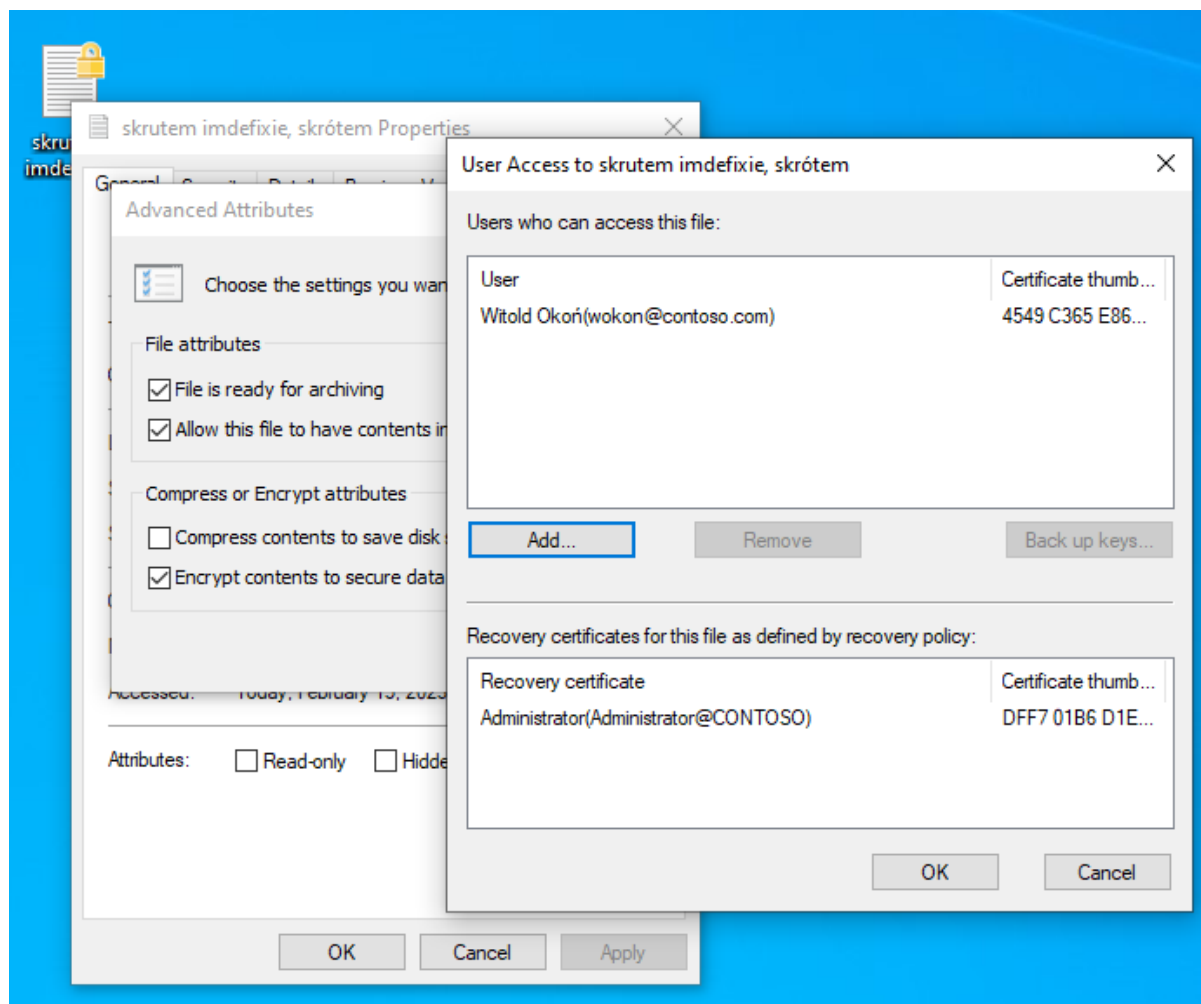
Automatycznie utworzono do tego certyfikat podpisany przez mój lokalny urząd certyfikujący.

Jako inny użytkownik (tutaj jgula) nie można otworzyć tego pliku:

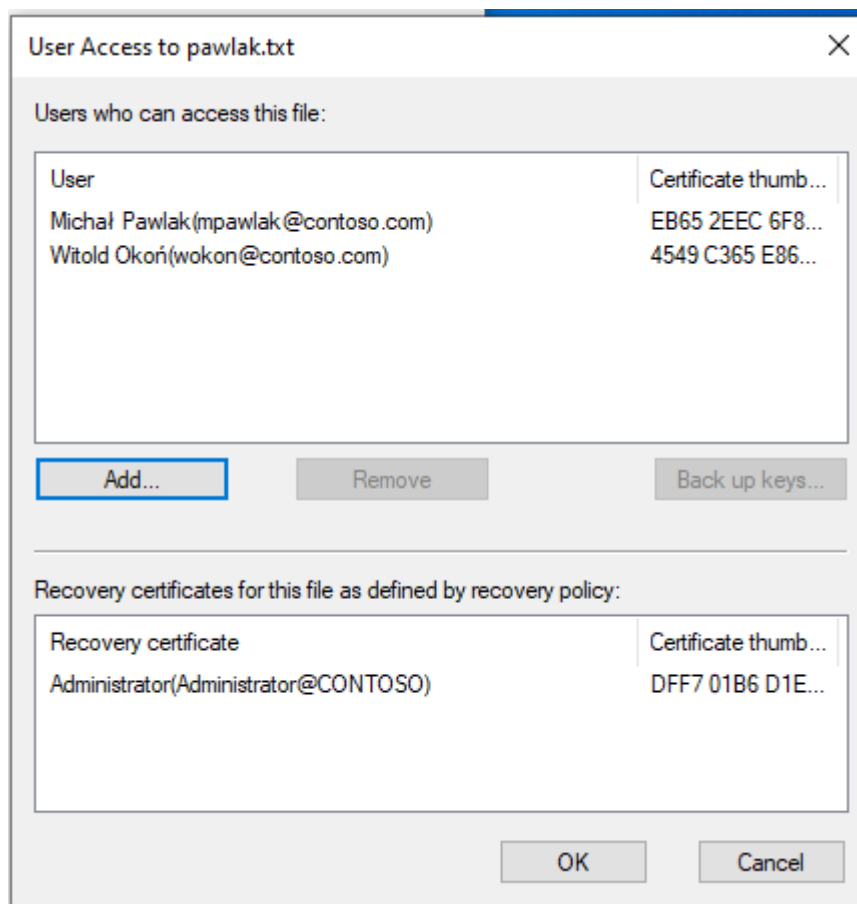
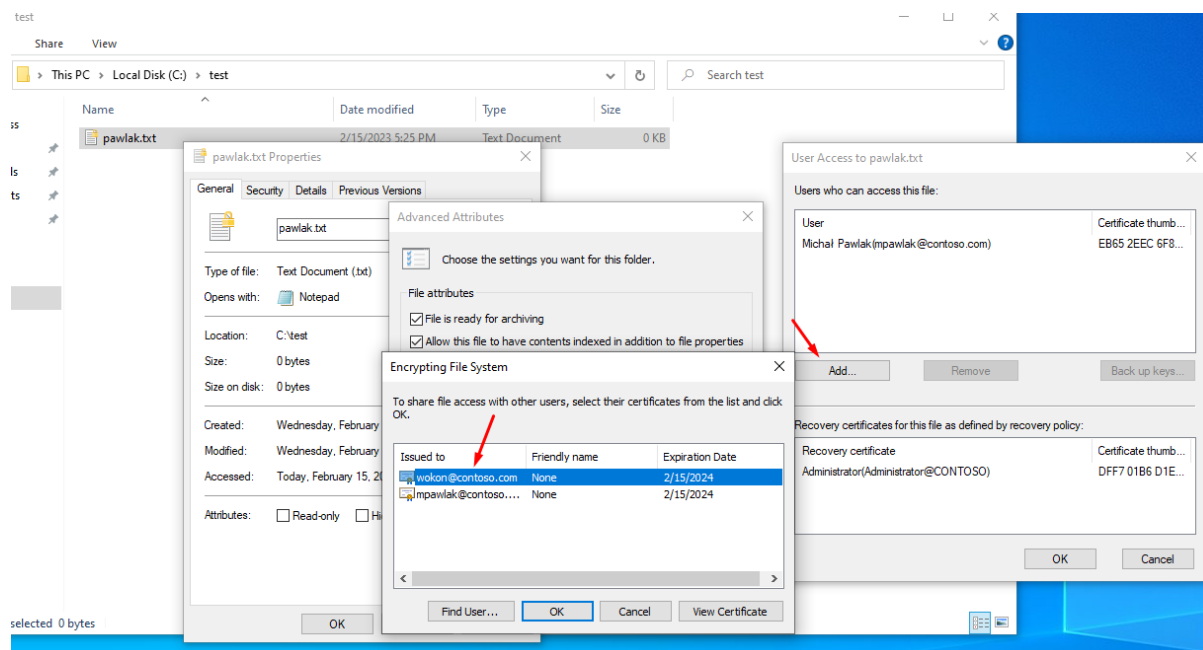


- Przetestować także możliwość nadania przez użytkownika "Imię Nazwisko" dostępu do zaszyfrowanego pliku dla innych użytkowników na przykładzie użytkownika *Witold Okoń*.

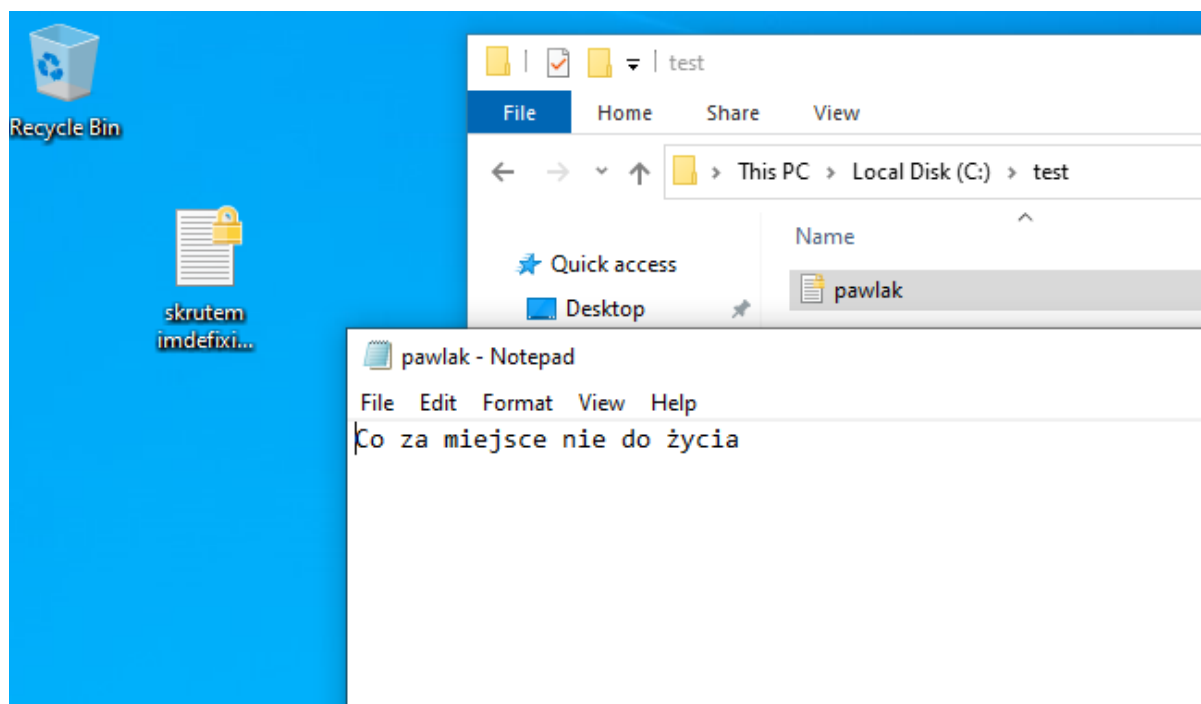
W pierwszej kolejności musimy wygenerować certyfikat dla wokon, dzięki któremu będzie można dać mu możliwość odszyfrowania pliku. Więc można na użytkowniku wykonać akcje z poprzedniego zadania, dzięki czemu wygeneruje się certyfikat automatycznie.



Teraz można dodać wokon do listy użytkowników którzy mają mieć dostęp do pliku pawlak.txt:



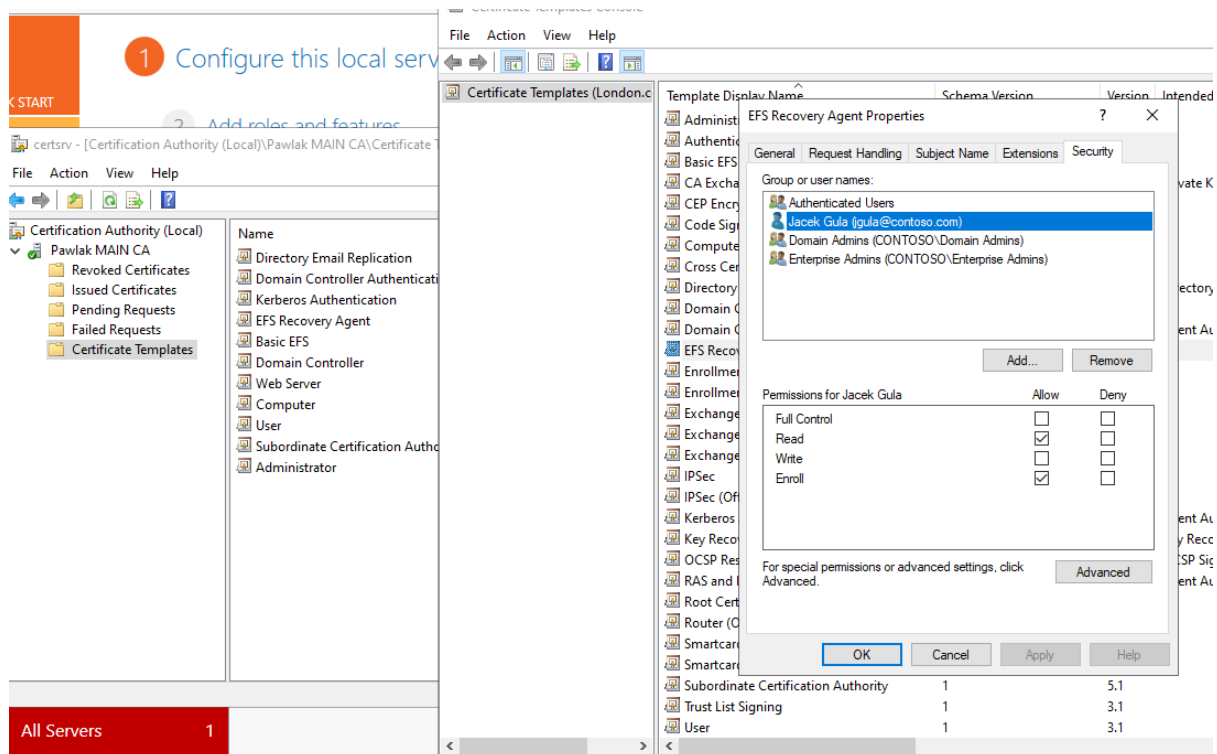
Sprawdzenie czy wokon może otworzyć plik:



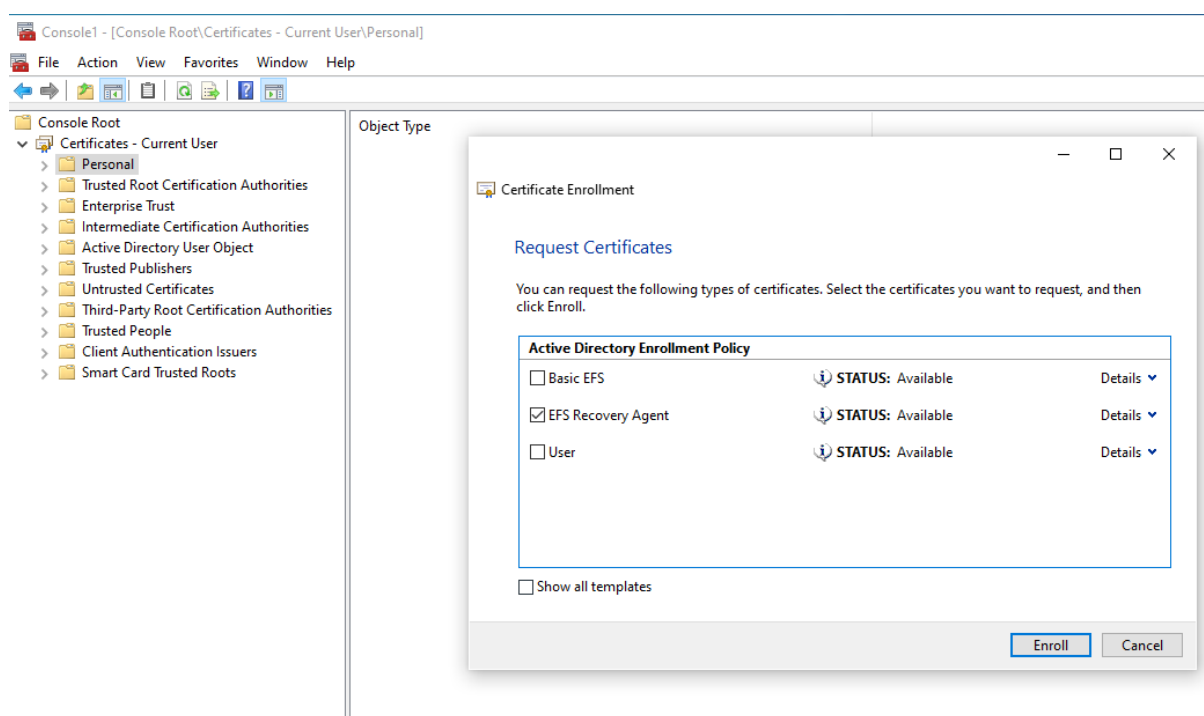
wokon może otwierać ten plik.

3. Pan *Jacek Gula* ma uzyskać "przymusowy" dostęp do wszystkich danych zaszyfrowanych w ramach systemu EFS na komputerach firmy, co należy wdrożyć, a następnie przetestować na przykładzie pliku "C:\test\{nazwisko}.txt".

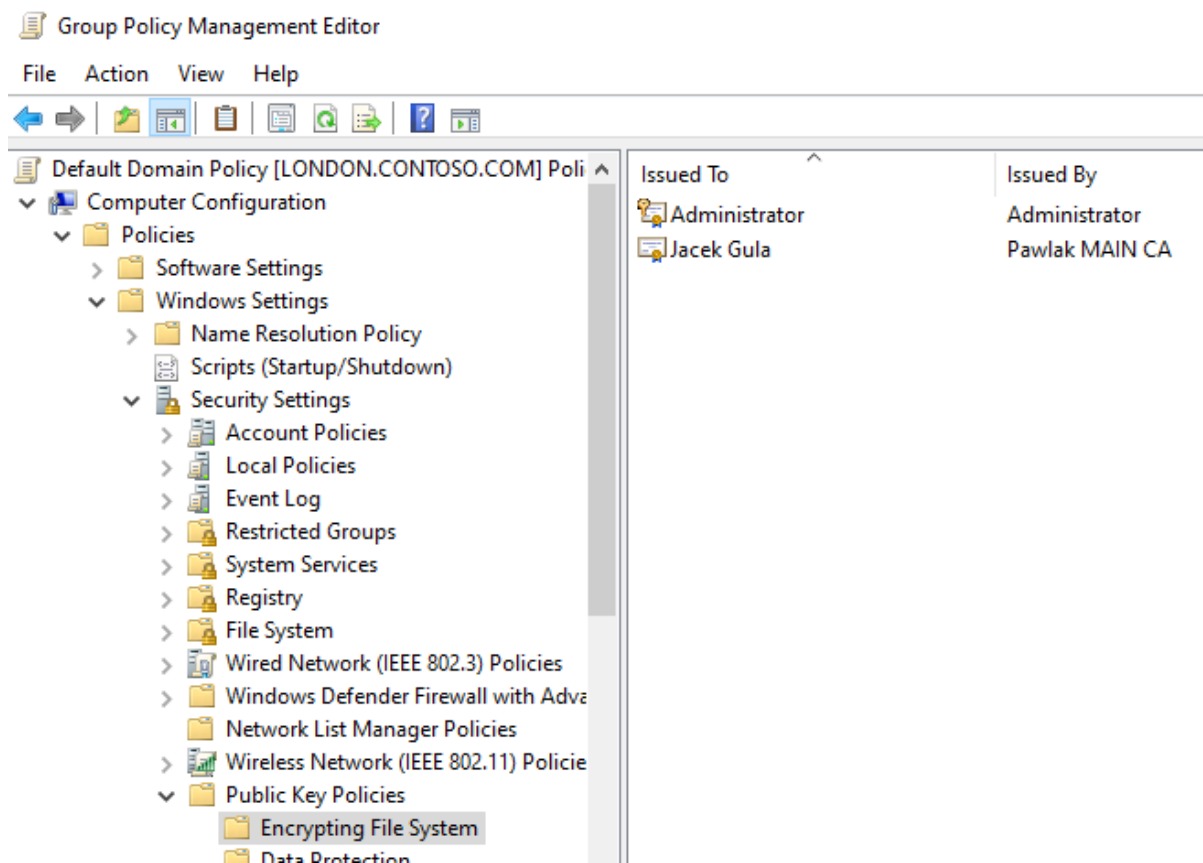
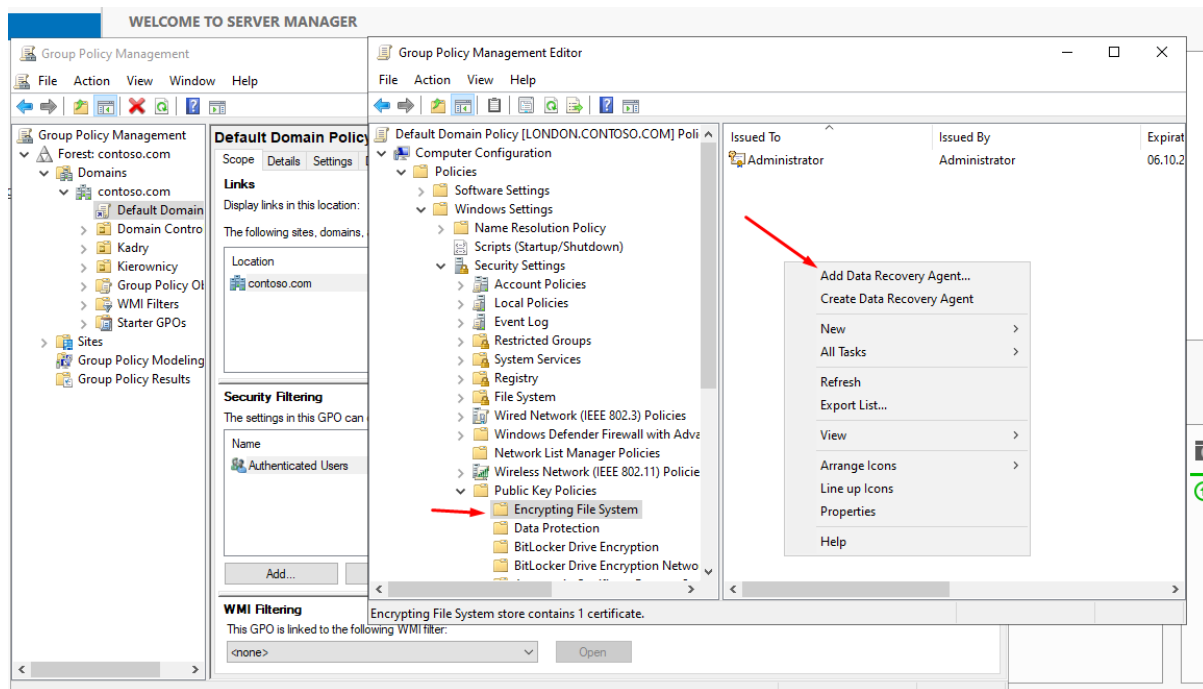
Trzeba dać mu możliwość wystąpienia o certyfikat "EFS Recovery Agent", następnie w Domyślnych zasadach domeny, dodać certyfikat jgula jako agenta odzyskiwania EFS



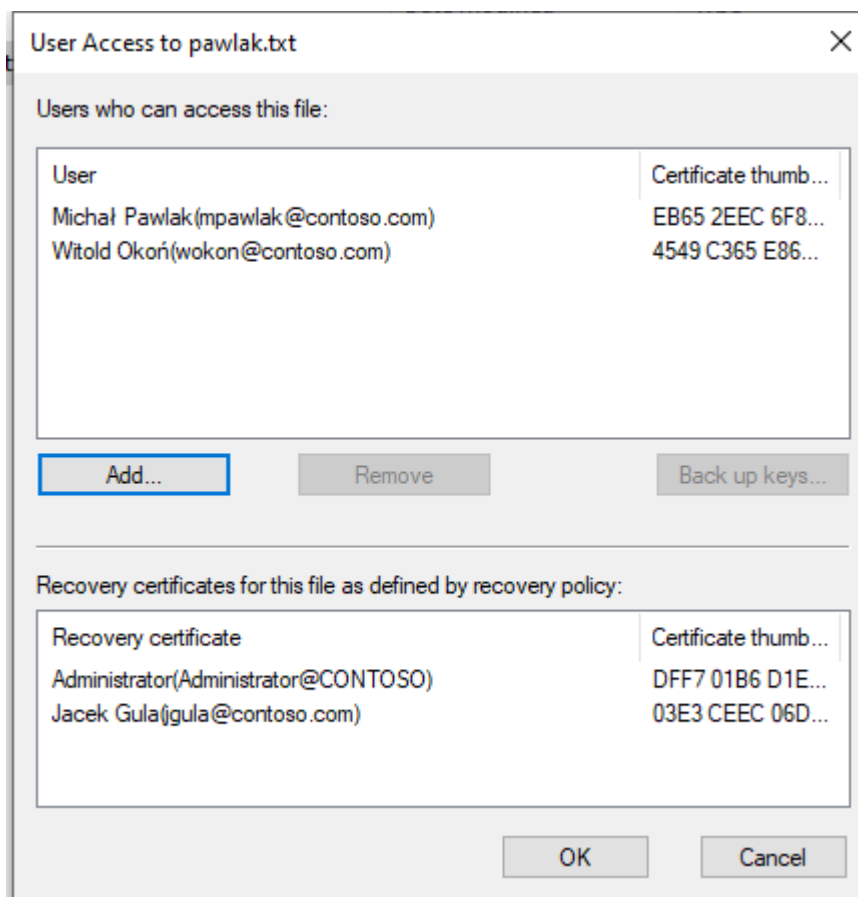
Teraz jgula może wystąpić o ten certyfikat lub można go wystawić w jego imieniu:



Dodanie go jako "Recovery Agent" w domenowych zasadach grup:



Po zaktualizowaniu zasad grupy na komputerze klienckim:



Jgula ma dostęp do pliku:

