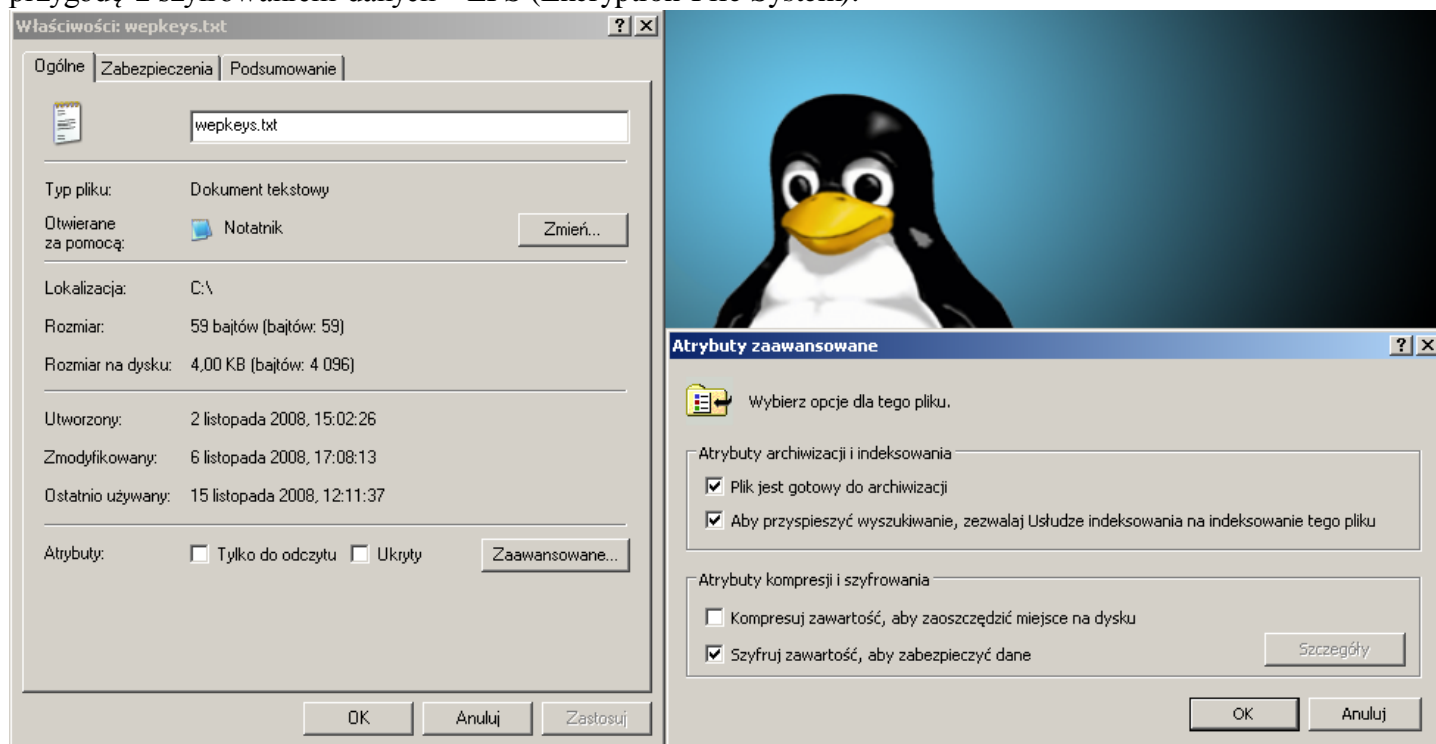


## T: Zabezpieczenia danych przy użyciu EFS.

**System utajniania plików (Encrypting File System - EFS)** wprowadza technologię szyfrowania plików magnetycznych, aby zapisywać na dysku zaszyfrowane pliki systemu plików Windows NT (NTFS). Używana technologia szyfrowania oparta jest na kluczach publicznych i działa jak zintegrowana usługa systemowa, co czyni ją łatwą w obsłudze, trudną do zaatakowania i przejrzystą dla użytkowników. Jeżeli użytkownik usiłujący dostać się do zaszyfrowanego pliku NTFS ma prywatny klucz do tego pliku, będzie mógł otworzyć plik i pracować z nimi przezroczyście jak z normalnym dokumentem. Użytkownik bez prywatnego klucza do pliku będzie miał dostęp zabroniony.

Windows XP w wersji Professional daje do ręki prostą w zastosowaniu technologię pozwalającą rozpocząć przygodę z szyfrowaniem danych - EFS (Encryption File System).

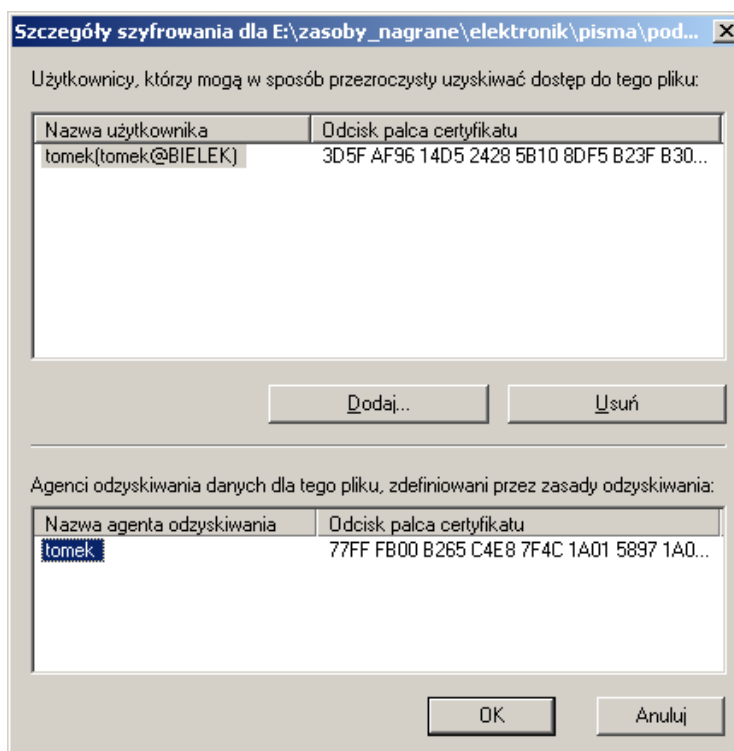


Po zaszyfrowaniu pliku można przejrzeć uprawnień do jego odszyfrowania użytkowników klikając szczegóły.

### Uwaga

- Polecenie wiersza poleceń **cipher** umożliwia konfigurację szyfrowania plików i katalogów (**cipher /r:nazwa\_pliku** - tworzenie nowego pliku certyfikatu oraz agenta odzyskiwania).
- Polecenie **certmgr.msc** uruchomi konsolę do zarządzania certyfikatami.
- Pod adresem [http://nazwa\\_serwera/certsrv](http://nazwa_serwera/certsrv) możliwe jest pozyskanie certyfikatów użytkownika.
- Polecenie **secpol.msc** uruchomi konsolę umożliwiającą dodanie agentów odzyskiwania danych.

EFS (Encrypted File System) – pozwala na szyfrowanie danych na dysku, co uniemożliwia odczytanie danych przez innych użytkowników lub danych z dysku na innym komputerze.

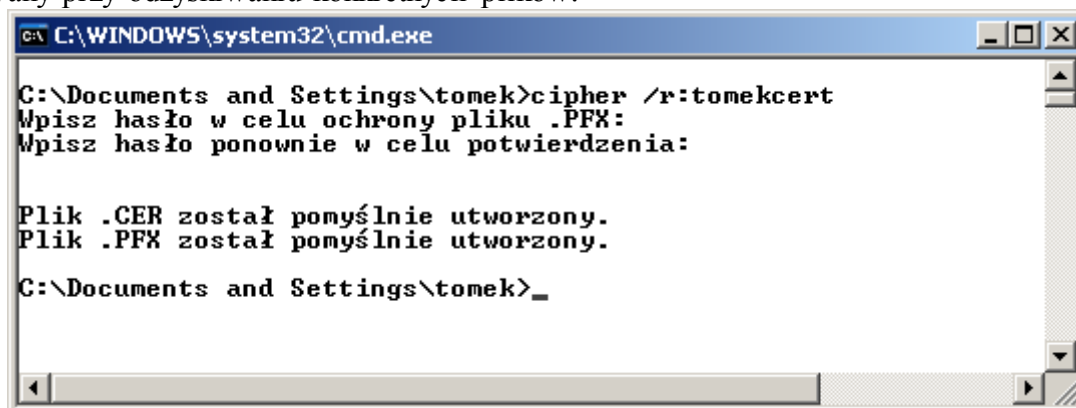


Funkcja EFS pozwala na szyfrowanie poszczególnych plików i folderów. Mechanizm ten jest oparty o szyfrowanie przy użyciu klucza publicznego. Funkcja EFS może korzystać z algorytmu szyfrowania Data Encryption Standard (DESX) lub Triple-DES (3DES). Pliki mogą być odszyfrowywane tylko przez upoważnionych użytkowników i wyznaczone osoby zajmujące się odzyskiwaniem danych. Inne konta systemowe z uprawnieniami dla danego pliku, nawet konto z uprawnieniami Przejęcie na własność, nie pozwalają na otwarcie pliku bez upoważnienia. Pliku nie można otworzyć nawet przy użyciu konta administratora, jeśli nie jest ono wyznaczone jako agent odzyskiwania danych. W przypadku próby otwarcia zaszyfrowanego pliku przez nieuprawnionego użytkownika nastąpi odmowa dostępu.

W wyniku wykonania polecenia **cipher /r:nazwa** powstaną dwa pliki:

- **nazwa.CER** gdzie zapisany zostanie nowy certyfikat,
- **nazwa.PFX** gdzie zapisany zostanie certyfikat i klucz prywatny agenta odzyskiwania,

Plik certyfikatu może zostać użyty przy tworzeniu zasad odzyskiwania plików EFS, natomiast plik klucza może być importowany przy odzyskiwaniu konkretnych plików.

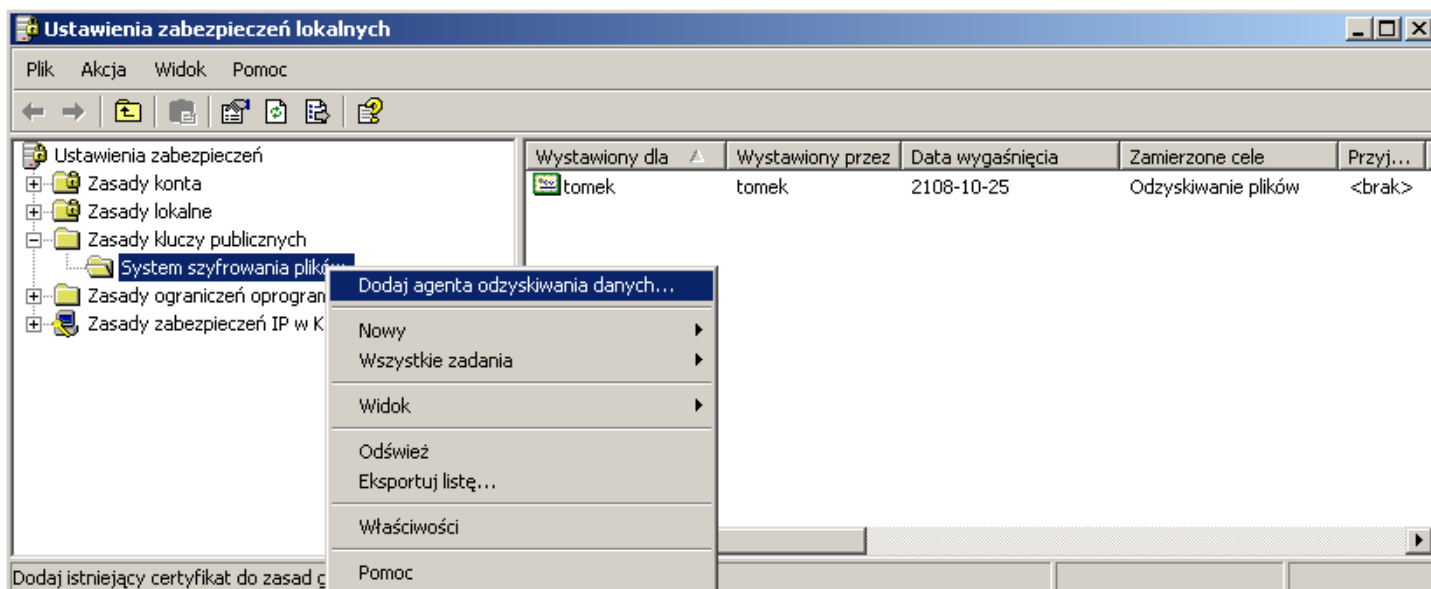


```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\tomek>cipher /r:tomekcert
Wpisz hasło w celu ochrony pliku .PFX:
Wpisz hasło ponownie w celu potwierdzenia:

Plik .CER został pomyślnie utworzony.
Plik .PFX został pomyślnie utworzony.

C:\Documents and Settings\tomek>_
```



Szyfrowanie z użyciem EFS (Encrypting File System):

- Operacje szyfrowania i deszyfrowania są przeprowadzane w tle i są niewidoczne dla użytkowników aplikacji. Podczas używania pliku jest on automatycznie deszyfrowany i szyfrowany ponownie podczas zapisu na dysk.
- EFS umożliwia dostęp do zaszyfrowanego pliku tylko autoryzowanemu użytkownikowi.
- Administrator może odzyskać plik zaszyfrowany przez dowolnego użytkownika.
- EFS posiada wbudowany system odzyskiwania danych. Z szyfrowania danych można korzystać wyłącznie jeśli w systemie istnieje przynajmniej jeden klucz odzyskiwania. EFS automatycznie generuje klucze odzyskiwania i umieszcza je w rejestrze systemu, gdy nie jest możliwy dostęp do domeny.
- Wymagany jest przynajmniej jeden agent odzyskiwania EFS. Można wyznaczyć dowolną liczbę agentów do zarządzania programem odzyskiwania EFS. Każdy agent wymaga posiadania certyfikatu EFS Recovery Agent.

- Szyfrowanie danych i ich kompresja wykluczają się wzajemnie. Niemożliwa jest bowiem kompresja danych zaszyfrowanych.
- Po zaszyfrowaniu folderu, pliki w nim zapisane będą automatycznie szyfrowane. Pliki szyfrowane są blokami, przy pomocy innych kluczy do szyfrowania każdego bloku. Do szyfrowania wykorzystywany jest szybki algorytm wykorzystujący klucze symetryczne. Klucze przechowywany jest w polu DDF (Data Decryption Field) oraz DRF (Data Recovery Field), znajdujących się w nagłówku pliku.
- Podczas otwierania zaszyfrowanego pliku, system EFS automatycznie wykrywa szyfrowanie i wyszukuje certyfikat użytkownika oraz powiązany z nim klucz prywatny. EFS wykorzystuje ten klucz do deszyfrowania pola DDF i odblokowania listy kluczy szyfrujących, co pozwala na jawne wyświetlenie zawartości pliku.
- Możliwa jest zmiana nazwy pliku po zaszyfrowaniu.
- Przy przenoszeniu pliku z folderu zaszyfrowanego do niezaszyfrowanego na tej samej partycji plik pozostaje zaszyfrowany.
- Dostęp do zaszyfrowanego pliku jest zakazany wszystkim użytkownikom, poza właścicielem klucza prywatnego. Tylko właściciel klucza lub agent EFS może odszyfrować plik. Użytkownik nie posiadający klucza prywatnego nie będzie mógł odczytać zawartości pliku nawet, gdy uzyska do niego dostęp (np. mając prawo Take Ownership).
- Jeśli klucz prywatny właściciela pliku jest niedostępny, agent odzyskiwania może otworzyć zaszyfrowany plik, wykorzystując swój klucz prywatny do pola DRF i odblokowując w ten sposób listę kluczy szyfrujących pliku.

Technologia ta opiera się o infrastrukturę klucza publicznego. Przy pomocy EFS-u możliwe jest zaszyfrowanie zarówno plików, jak i folderów. W procesie tym wykorzystany jest algorytm 3DES bądź AES - w zależności od wersji OS-a (XP - 3DES, XP SP1 w górę AES). EFS może skorzystać z certyfikatów typu self signed lub wygenerowanych przez Urząd Certyfikacji - jeżeli takowy jest zainstalowany w środowisku. Dzięki wykorzystaniu certyfikatów EFS przywiązuje zaszyfrowane pliki do konkretnego użytkownika zalogowanego w systemie. To z kolei sprawia, że po zalogowaniu się użytkownik będący twórcą zaszyfrowanego pliku uzyskuje prawo automatycznej deszyfracji. Z punktu widzenia użytkownika EFS jest więc w zasadzie w pełni przezroczysty. Jedynym sygnałem świadczącym o objęciu pliku czy katalogu szyfrowaniem jest oznaczenie go przez system (domyślnie) kolorem zielonym, co ułatwia orientację.

Mimo, że rozpoczęcie samego procesu szyfrowania (patrząc oczami użytkownika) jest proste, zanim je uruchomimy warto mieć świadomość tego, dlaczego EFS nie jest systemem idealnym i jakie są jego podstawowe słabości. Do EFS-u można mieć wiele zastrzeżeń, ale - jak mówią grzybiarze - lepszy rydz niż nic. Poza tym od czegoś trzeba zacząć. Jak już wspomnieliśmy, EFS należy do grupy rozwiązań pozwalających użytkownikom szyfrować tylko i wyłącznie pliki i foldery. Nie przeciwdziała on uruchomieniu systemu operacyjnego przez osobę nieuprawnioną. Poza tym, mimo, że zaszyfrowane mogą być zarówno foldery i pliki, to i tak nie wszystkie. Nie ma możliwości objęcia **"enkrypcją"** informacji przechowywanych w folderze systemowym. EFS nie poradzi sobie także z innymi plikami, które zostały oznaczone jako systemowe.

Możemy więc śmiało zapomnieć o zaszyfrowaniu takich informacji jak plik hibernacyjny, czy stronicowania. Podobnie będzie, jeżeli zechcemy spakować plik zaszyfrowany - EFS nie obsługuje takiej operacji. Inny problem polega na tym, że w zasadzie szyfrowany jest nie sam plik, ale jego zawartość. Wszelkie meta dane przywiązane do pliku czy np. rozmiar, czy data utworzenia można bez problemu uzyskać. Podobnie rzecz ma się z katalogami. Będąc dowolnym, zalogowanym użytkownikiem możemy bez problemu podejrzeć zawartość katalogu. Przy okazji warto tutaj podkreślić, że kluczowe dla skuteczności ochrony realizowanej przez EFS jest silne hasło użytkownika. Jeżeli osoba nieuprawniona zdobędzie hasło, to będzie to równoznaczne z uzyskaniem prawa odszyfrowania pliku. Następna bolączka wynika z przywiązania mechanizmu EFS do systemu plików NTFS.

Możliwe jest także współdzielenie zaszyfrowanych plików pomiędzy użytkownikami. Wymaga to dwóch rzeczy - posiadania przez innego użytkownika certyfikatu oraz przypisania tegoż certyfikatu do pliku po jego zaszyfrowaniu. Należy więc najpierw zaszyfrować plik, a dopiero potem w jego właściwościach w zakładce "Zaawansowane" kliknąć "Szczegóły" i dodać uprawnionych użytkowników.

Po wykonaniu pierwszej operacji zaszyfrowania pliku/katalogu wygenerowany zostanie certyfikat dla użytkownika, który rozpoczął proces. Dobrze jest wykonać jego kopię np. na nośnik zewnętrzny. Należy uruchomić konsolę MMC (Start => Uruchom => mmc), dodać przystawkę Certyfikaty (Plik => Dodaj/Usuń przystawkę => Dodaj => Certyfikaty => Moje konto użytkownika). Następnie odszukać certyfikat i wykonać polecenie "Eksportuj" z menu "Akcja => Wszystkie zadania". Wyeksportowany w ten sposób klucz należy przechowywać w bezpiecznym miejscu.

W usłudze Active Directory możliwe jest wykorzystanie konsoli administracyjnej **Szablony certyfikatów (certtmpl.msc)** do aktualizacji, instalacji lub usuwania szablonów certyfikatów używanych na serwerze. Za pomocą konsoli możemy również wykonać zadanie **Zarejestruj ponownie wszystkich posiadaczy certyfikatów**.

#### Źródło:

<http://www.networld.pl/news/132378/Szyfrowanie.danych.w.Windowsie.XP.bez.dodatkowych.narzedzi.html>

System EFS umożliwia nam stworzenie tzw. **Agenta odzyskiwania danych**, który w momencie gdy utracimy certyfikat szyfrowania pliku i skojarzony z nim klucz prywatny umożliwi nam dostęp do zaszyfrowanych informacji.

Cały etap tworzenia agenta odzyskiwania zaszyfrowanych danych rozpoczniemy od stworzenia specjalnego certyfikatu, który następnie desygnujemy użytkownikowi, który będzie mógł w razie jakiegokolwiek zagrożenia utraty zabezpieczonych plików po prostu nam je odzyskać - czyli będzie spełniał rolę **agenta odzyskiwania danych**. Proces ten jest bardzo prosty i wygląda następująco:

- Logujemy się na komputerze, na którym znajdują się zabezpieczone wcześniej informacje jako **Administrator**.
- Klikamy **Start, Uruchom...** i w polu tekstowym okna, które się wyświetli wpisujemy polecenie **cmd**, które uruchomi nam wiersz poleceń.
- Następnie wpisujemy **cipher /r:nazwa\_pliku** i podajemy hasło, które będzie chroniło utworzone pliki. W tym momencie stworzone zostają dwa pliki o rozszerzeniach \*.pfx i \*.cer (gdzie \* to zadeklarowana przez nas wcześniej nazwa\_pliku). Z racji tego, że osoby które uzyskają dostęp do stworzonych przed chwilą dokumentów jednocześnie nabywają prawa agenta odzyskiwania danych, radzimy zachować je w bezpiecznym miejscu, najlepiej na dyskiecie, a ich odpowiedniki usunąć z dysku twardego.

Kolejnym krokiem prowadzącym do stworzenia wspomnianego wcześniej agenta będzie **desygnacja agenta odzyskiwania danych**. Jak już wspomnieliśmy agentem tym może zostać każdy użytkownik - zarówno ten, który korzysta z tego samego komputera jak i ten, który jest użytkownikiem tej samej domeny. Odradzamy jednak użycia konta, z którego zostały zaszyfrowane dane jako agenta, ponieważ takie ustawienie do niczego nie prowadzi. Mianowicie w takiej sytuacji w momencie gdy profil ten zostanie uszkodzony lub usunięty, tym samym tracimy wszystkie klucze pozwalające na deszyfrację zabezpieczonych danych. Proces desygnacji prezentuje się następująco: logujemy się na konto użytkownika, który ma zostać agentem odzyskiwania danych, klikamy **Start, Uruchom...** i wpisujemy polecenie **certmgr.msc**, które uruchomi nam konsolę odpowiedzialną za zarządzanie certyfikatami. Klikamy **Certyfikaty - Bieżącego użytkownika**, a następnie **Osobisty** i wybieramy polecenie **Akcja, Wszystkie zadania i Importuj**. W tym momencie ukaże się naszym oczom **Kreator importu certyfikatu**, który poprowadzi nas poprzez cały etap importowania certyfikatu z pliku, który stworzyliśmy kilka minut temu. W pierwszym oknie kreatora nasze działanie ogranicza się do kliknięcia przycisku **Dalej**. W kolejnym natomiast wskazujemy ścieżkę, gdzie znajduje się jeden z wcześniej stworzonych plików o rozszerzeniu \*.pfx. Aby tego dokonać klikamy **Przełóż...** i w polu **Pliki typu:** wybieramy opcję **Wymiana informacji osobistych (\*.pfx; \*.p12)**. Następnie zostajemy poproszeni o podanie hasła, które wpisaliśmy podczas procesu tworzenia wspomnianych już plików. Zaznaczamy opcję **Oznacz ten klucz jako eksportowalny** oraz klikamy przycisk **Dalej**, kończąc pracę na tym etapie importu certyfikatu. Kreator poprosi nas o wybór **Magazynu certyfikatów**, ograniczymy się tutaj do automatycznego zaznaczenia kreatora zaznaczając opcję **Automatycznie wybierz magazyn certyfikatów na podstawie typu certyfikatów** a w kolejnych krokach kliknijmy klikając **Dalej** oraz **Zakończ**. Naszym następnym ruchem powinno być uruchomienie okna dialogowego **Ustawienia zabezpieczeń lokalnych**. Kliknijmy w tym celu po raz kolejny **Start, Uruchom...** i wpiszmy w polu tekstowym polecenie **secpol.msc**. W nowym oknie przechodzimy kolejno do: **Ustawienia zabezpieczeń, Zasady kluczy publicznych i System szyfrowania plików**. Wybieramy

polecenie **Akcja, Dodaj agenta odzyskiwania danych** i poprzez kliknięcie **Dalej** przechodzimy do kolejnego etapu, gdzie naszym zadaniem będzie wskazanie ścieżki pod którą znajduje się stworzony przez nas na początku plik o rozszerzeniu **\*.cer.** Na liście agentów odzyskiwania pojawi się użytkownik, zdefiniowany jako **USER\_UNKOWN**, klikamy kolejno **Dalej** i **Zakończ**. Operacja, którą przed momentem sfinalizowaliśmy sprawiła, iż bieżący użytkownik, na koncie którego cały ten proces miał miejsce - jest od tego momentu agentem odzyskiwania plików i co za tym idzie ma dostęp do zabezpieczonych przez nas informacji.

**Źródło:**

[http://www.centrumxp.pl/WindowsXP/1131,1,Tworzenie\\_agenta\\_odzyskiwania\\_danych.aspx](http://www.centrumxp.pl/WindowsXP/1131,1,Tworzenie_agenta_odzyskiwania_danych.aspx)

**Więcej informacji na stronach:**

<http://technet2.microsoft.com/windowsserver/pl/library/e98be8eb-7104-4a68-8e1a-dc3d799c75b41045.msp?mfr=true>

[http://technet.microsoft.com/pl-pl/library/cc738530\(WS.10\).aspx](http://technet.microsoft.com/pl-pl/library/cc738530(WS.10).aspx)

<http://wampir.mroczna-zaloga.org/archives/928-efs-odzyskiwanie-zaszyfrowanych-plikow.html>