POLITECHNIKA CZĘSTOCHOWSKA
WYDZIAŁ INŻYNIERII MECHANICZNEJ I INFORMATYKI

Sprawozdanie

System szyfrowania plików i katalogów EFS

Piotr Zyszczak i Damian Łukasik

Nr albumu: 113066/112993

Kierunek: Informatyka

Studia: stacjonarne

Poziom studiów: II

Częstochowa, 2015

Spis treści

1 Cel i zakres zajęć **3**

2 Wstęp teoretyczny **4**

3 Przebieg **5**

4 Wnioski **6**

1. Cel i zakres zajęć

Przy pomocy dwóch kont użytkowników należało przetestować działanie systemu EFS. Należało zaszyfrować plik na 1 użytkowniku i sprawdzić na innym koncie czy się otwiera, a potem sprawdzić

2. Wstęp teoretyczny

System szyfrowania plików (EFS, Encrypting File System) jest funkcją systemu Windows pozwalającą na przechowywanie danych na dysku twardym w postaci zaszyfrowanej. Szyfrowanie jest najwyższym stopniem ochrony dostępnym w systemie Windows w celu zapewnienia bezpieczeństwa informacji.

Główne funkcje systemu EFS:

- Szyfrowanie jest proste; aby je włączyć, wystarczy zaznaczyć pole wyboru we właściwościach pliku lub folderu.
- Użytkownik decyduje, kto może odczytać pliki.
- Pliki są szyfrowane po ich zamknięciu, ale automatycznie gotowe do użycia po ich otwarciu.
- Jeśli plik nie ma być dłużej szyfrowany, należy wyczyścić pole wyboru we właściwościach pliku.

3. Przebieg

Ćwiczenie zaczęliśmy od zaszyfrowania pliku przy wykorzystaniu opcji wbudowanej w system. Czyli po prostu należało wejść we właściwości a tam zaawansowane, gdzie otwierają się opcje kompresji i szyfrowania (trzeba pamiętać że się wzajemnie wykluczają). Klikamy szyfrowanie. W trakcie zatwierdzania zmian windows zapyta o to m.in. czy chcemy zaszyfrować katalog,wykonać kopię kluczy(za pierwszym razem), czy szyfrujemy wszystkie pliki czy tylko jeden.

Następnie logujemy się jako 2 użytkownik i oczywiście dostajemy odpowiedź odmowną ponieważ nie mamy dostępu do klucza prywatnego.

Kolejnym krokiem będzie sprawienie by plik się otworzył. Logujemy się na 1 koncie i otwieramy program MMC . Dodajemy przyssawkę Certyfikaty, następnie otwieramy katalog z certyfikatami osobistymi. Potem klikamy wszystkie zadania i eksportuj.

W ten sposób otworzymy Kreator eksportu certyfikatów. Na kolejnej stronie kreatora należy zaznaczyć opcję eksportu klucza prywatnego. Na kolejnych stronach należy podać hasło. Następnie należy wybrać plik docelowy. Po poprawnym wykonaniu tych operacji otrzymamy plik z kopią klucza prywatnego. Klucz ten można następnie przechowywać jako kopię zapasową lub zaimportować u innego użytkownika (co zamierzamy zrobić).

Ostatnim krokiem jest import certyfikatu na koncie 2 użytkownika poprzez Centrum importu certyfikatów. Przy okazji podajemy hasło ustalone wcześniej.

4. Wnioski

Plik został zaszyfrowany i odszyfrowany poprawnie.