



Zastosowanie Encrypting File System

Konrad Sagała
MCSE



Agenda

- ◆ Jak działa EFS
- ◆ Podstawy odzyskiwania danych
- ◆ Scenariusz dla Windows 2000 Standalone
- ◆ Scenariusz dla domeny Windows 2000
- ◆ Zmiany w systemie .NET
- ◆ Scenariusz dla systemu .NET
- ◆ Zalecenia



Encrypting File System

- ◆ Prywatność danych bez potrzeby dodatkowego zarządzania
 - Zabezpieczenie danych na komputerach przenośnych
 - Możliwość konfigurowanego odzyskiwania danych
- ◆ Integracja z podstawowymi komponentami systemu
 - System plików NTFS
 - Polityka LSA
 - Zarządzanie kluczami Crypto API
- ◆ Wysoka wydajność działania niewidoczna dla użytkownika



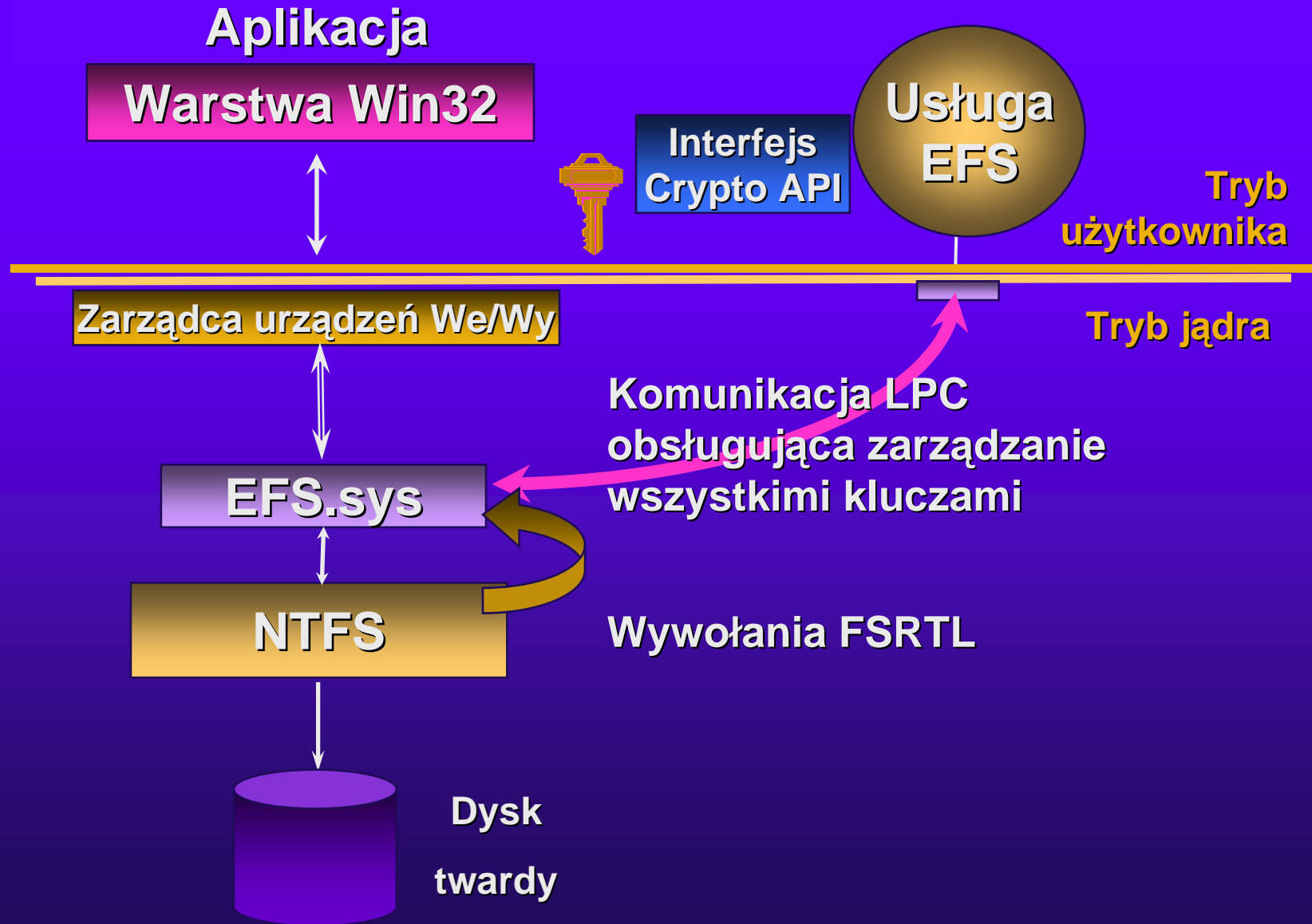
Jak działa EFS



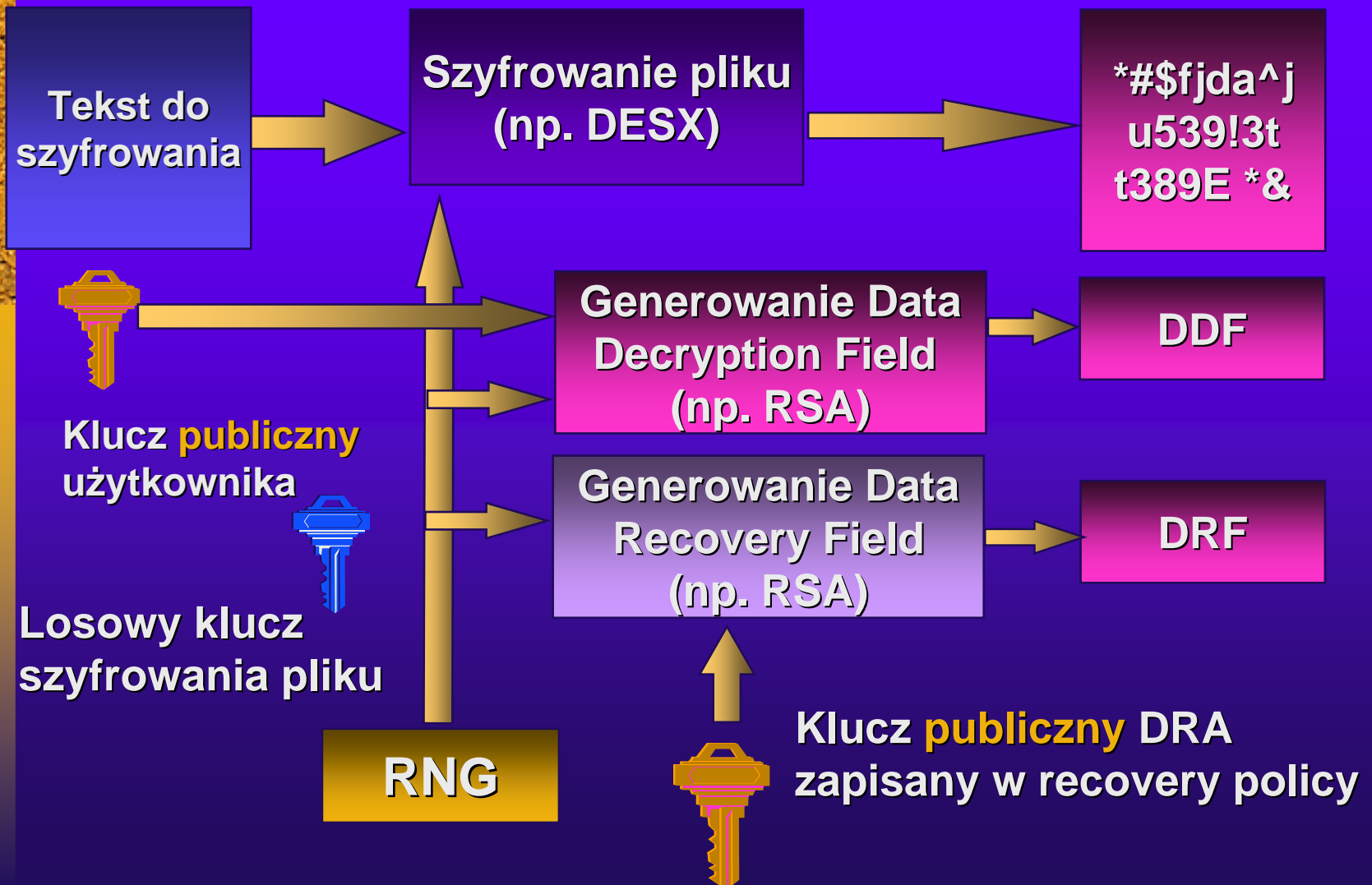
EFS – podstawowe fakty

- ◆ System EFS stosuje szyfrowanie kluczem symetrycznym w połączeniu z technologią klucza publicznego
- ◆ Dostęp do zaszyfrowanego pliku
 - Użytkownik, który zaszyfrował plik
 - Agent odzyskiwania - DRA (Data Recovery Agent)

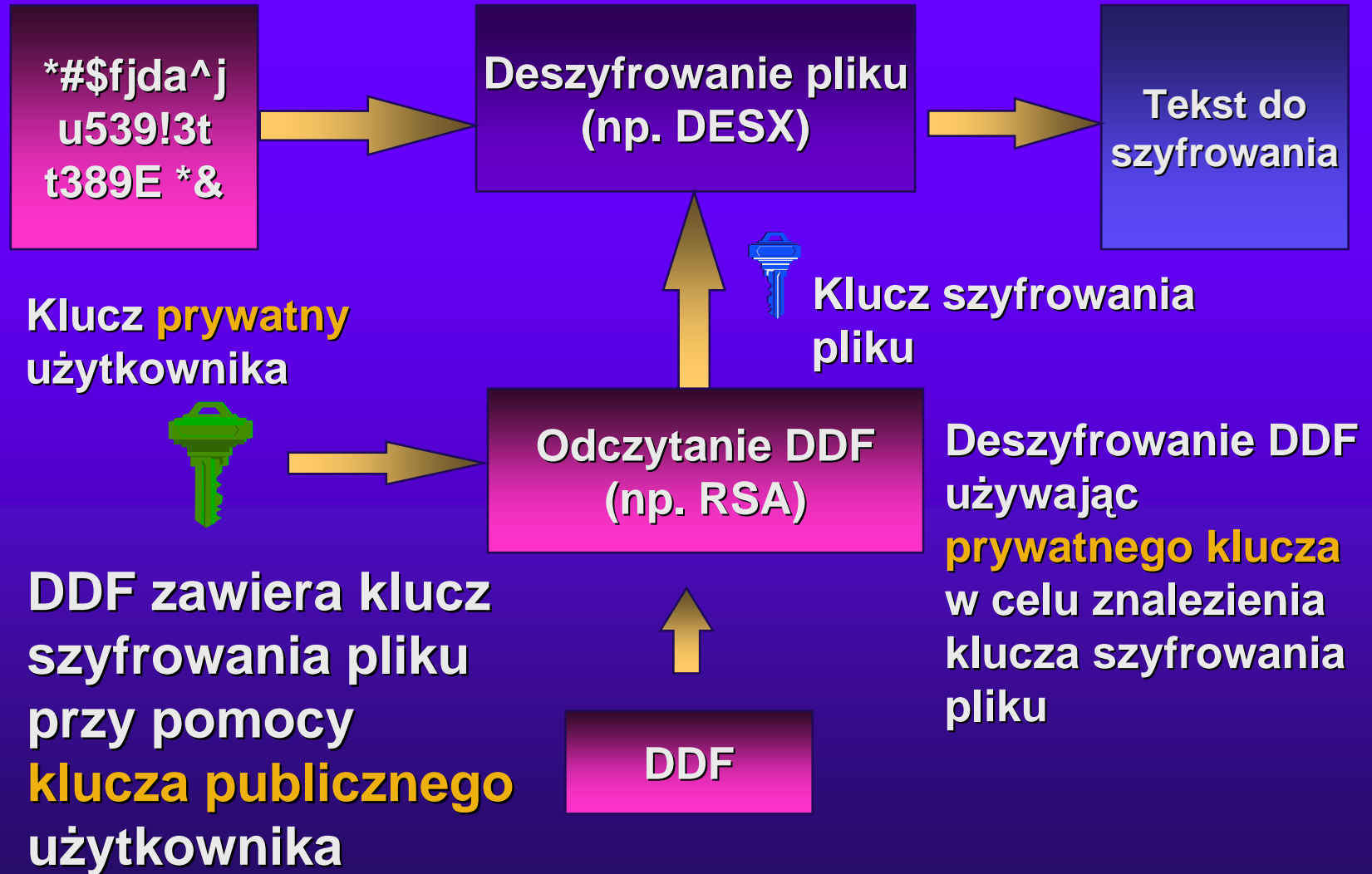
Architektura systemu EFS



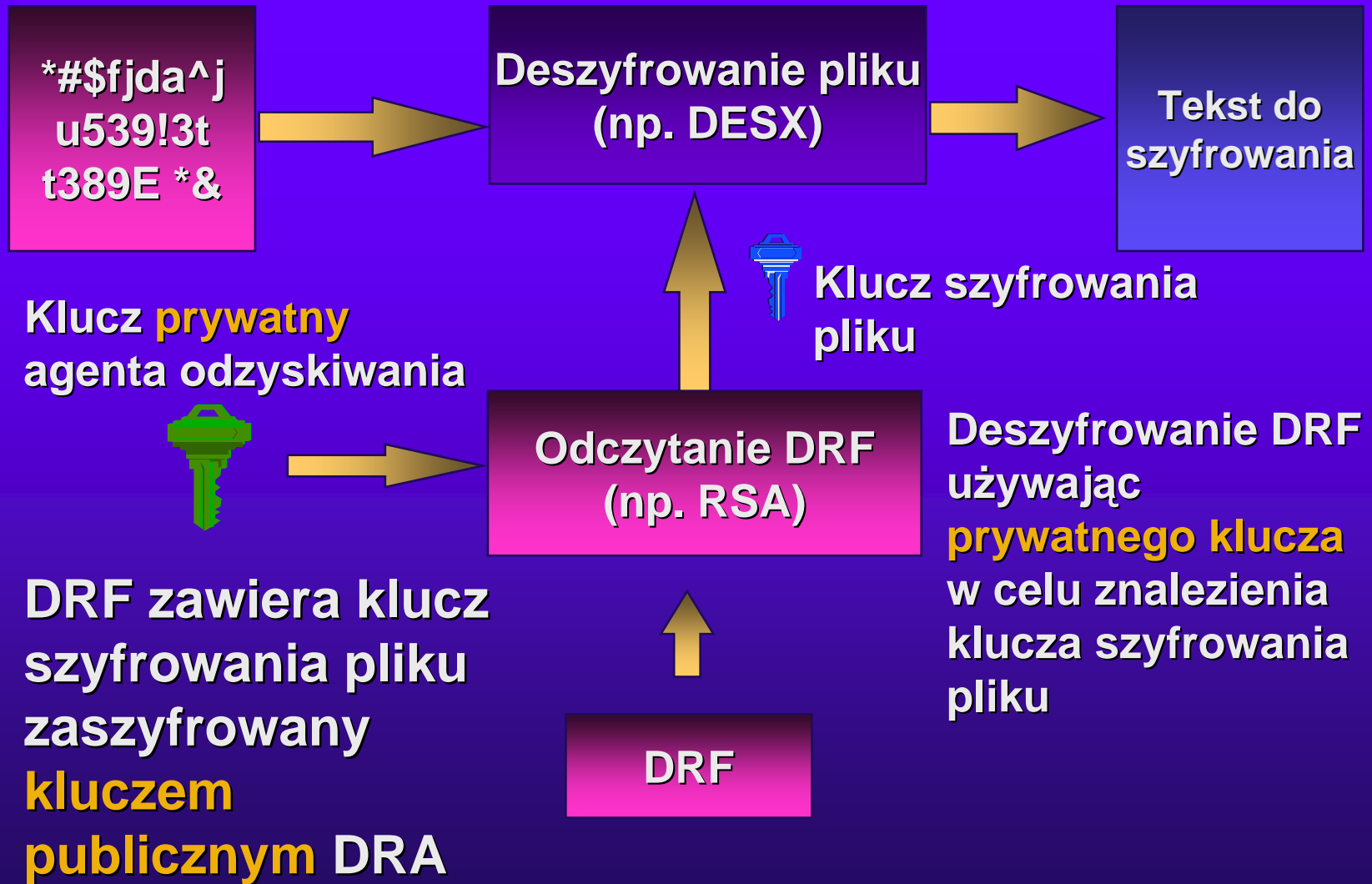
Szyfrowanie pliku



Deszyfrowanie pliku



Odtwarzanie pliku





Informacje o pliku

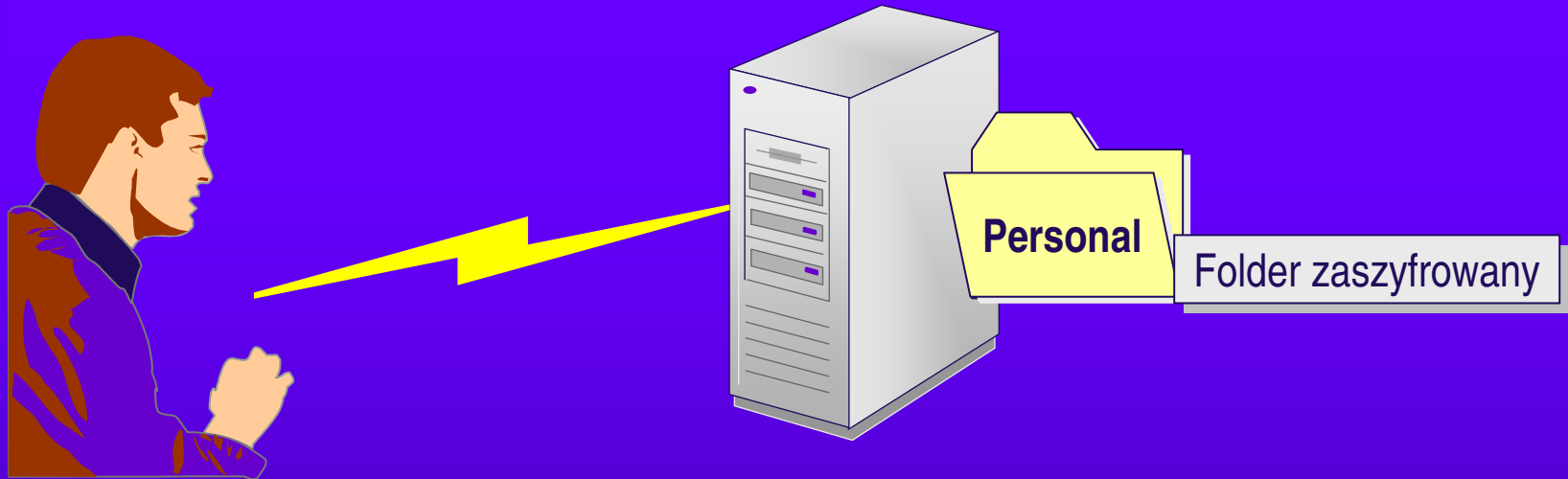
- ◆ W celu sprawdzenia właściwości zaszyfrowanego pliku i właściwego dla niego agenta odzyskiwania używamy `efsinfo.exe`
 - `Efsinfo /R /U <filename>`
- ◆ Dokładny opis programu – Knowledgebase Article Q243026



Pliki szyfrowane na serwerze

- ◆ Należy spełnić następujące warunki:
 - Domena Windows 2000 lub .NET
 - Konto serwera musi być zaufane do delegacji w Active Directory
 - system plików NTFS
 - Użytkownik musi posiadać konto w Active Directory

Pliki szyfrowane na serwerze



- ◆ Profil użytkownika istnieje na zdalnym serwerze
- ◆ Serwer wykorzystuje profil poprzez delegację Kerberos



Pliki szyfrowane na serwerze

- ◆ Profil użytkownika jest dostępny na dwa sposoby:
 - ładowany jest zdefiniowany profil wędrujący użytkownika
 - Serwer generuje nowy profil lokalny
- ◆ Do zapamiętania
 - Profile użytkowników uwzględniamy w polityce backupowej
 - Jeżeli prywatny klucz jest generowany na serwerze, to jest to jego jedyna kopia!



Zalecenia

- ◆ W polityce backupowej uwzględniamy pełny system oraz profile użytkowników
- ◆ Wykorzystujemy profile wędrujące
- ◆ Włączamy opcję „Trusted for Delegation” na wybranych serwerach
- ◆ Więcej szczegółów - Knowledgebase Article Q283223



Podstawy odtwarzania zaszyfrowanych plików



Definiowanie Zasad Odzyskiwania

◆ Recovery Agent Policy

- Definiowanie jednego lub kilku agentów odtwarzania
- Domyślnie konto „Administrator”
 - pierwsze konto administracyjne na stacji/serwerze (tryb wolnostojący)
 - Konto administratora na pierwszym DC zainstalowanym w domenie

◆ Pusta zasada odzyskiwania

- Wyłącza EFS w Windows 2000
- Brak agentów odtwarzania = Brak EFS



Definiowanie Zasad Odzyskiwania

◆ Brak zasad odzyskiwania

- Używane w przypadkach kiedy polityka bezpieczeństwa nie zezwala na stosowanie kont odzyskiwania
- EFS uruchomiony lokalnie i niezdefiniowane Zasady Grupowe w domenie AD
- Na lokalnym komputerze klucz prywatny DRA skasowany



Zmiany polityki

- ◆ W momencie wyłączenia EFS:
 - użytkownik może otworzyć wcześniej zaszyfrowane pliki
 - użytkownik nie może zmodyfikować zaszyfrowanego pliku
 - użytkownik nie może szyfrować nowych plików
 - modyfikowany plik musi być zapamiętany w postaci niezaszyfrowanej



Generowanie certyfikatów odzyskiwania dla EFS

- ◆ Lokalny administrator na pierwszym kontrolerze w domenie staje się automatycznie agentem odzyskiwania
- ◆ Wymagany jest Korporacyjny Urząd Certyfikujący Windows 2000/.NET



Import/Export certyfikatów

- ◆ Można pracować z wcześniej istniejącymi certyfikatami i parami kluczy
 - Poprzez konsolę MMC Certyfikaty wybieramy opcję eksport/import kluczy prywatnych
 - zaznaczamy opcję „Delete the private key if the export is successful”
 - przechowujemy klucz w bezpiecznym miejscu
 - do odzyskania pliku na dowolnym komputerze importujemy plik .pfx z kluczem tą samą konsolą



Scenariusz dla Windows 2000 standalone



Ten scenariusz dotyczy:

- ◆ Komputerów Windows 2000/XP w grupie roboczej
- ◆ Komputerów Windows 2000/XP w domenie NT
- ◆ Komputerów Windows 2000/XP w innym środowisku sieciowym



Kluczowe zagadnienia

- ◆ Brak centralnego agenta odzyskiwania
- ◆ EFS dostępny tylko na wersji „biurowej” oprogramowania (nie występuje w XP Home Edition)
- ◆ Lokalne konto administratora jest agentem odzyskiwania
 - potencjalne źródło ataków
- ◆ Brak centralnej bazy kluczy



Zalecenia

- ◆ Należy usunąć klucz DRA z komputera i przechowywać osobno
- ◆ Należy archiwizować klucze prywatne użytkowników
- ◆ Dobrze jest skonfigurować SYSKEY w celu zabezpieczenia systemu
- ◆ Należy pamiętać, że dołączenie do domeny AD zmienia DRA
- ◆ Należy wymusić na użytkownikach stosowanie silnych haseł



Scenariusz dla domeny Windows 2000



Domyślny scenariusz

- ◆ Konto administratora domeny jest domyślnym DRA
 - Prywatny klucz odzyskiwania EFS w domenie przechowywany jest w lokalnym profilu administratora na pierwszym kontrolerze domeny zainstalowanym w domenie
- ◆ DRA jest zdefiniowany w GPO „domyślne zasady domenowe”



Zalecenia

- ◆ Należy zawsze konfigurować notebooki jako stacje domeny Windows 2000
- ◆ Najlepiej jest zdefiniować osobny OU dla notebooków i delegować dla niego oddzielnego DRA
- ◆ Należy domyślnie włączać szyfrowanie folderów takich jak Moje Dokumenty
- ◆ Dla zwiększenia bezpieczeństwa stosować syskey



Zalecenia

- ◆ W celu uruchomienia EFS dla wybranej grupy komputerów domeny należy:
 - Zdefiniować agenta odzyskiwania EFS na poziomie OU
 - Przenieść komputery do tego OU
 - Usunąć politykę odzyskiwania na poziomie domeny



Zmiany w .NET



Zmiany w modelu odzyskiwania

◆ Model domenowy

- brak wymagań dla DRA
- może działać bez polityki odzyskiwania danych
- administrator domeny jest domyślnym DRA

◆ Domeny NT 4.0 i serwery wolnostojące

- brak domyślnych agentów odzyskiwania
- agent musi być stworzony komendą „cipher.exe /R”



Rozszerzenia EFS

- ◆ Pliki zaszyfrowane zaznaczone są innym kolorem
- ◆ Przy korzystaniu z folderów offline pliki są przechowywane w szyfrowanej bazie danych
- ◆ Rozszerzony model kryptograficzny
 - algorytm 3DES



EFS i WebDAV

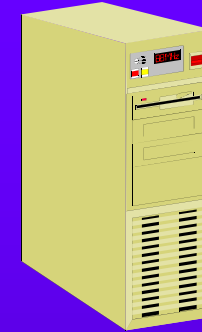
- ◆ Możliwość szyfrowania plików na serwerach internetowych - integracja EFS z usługą WebDAV
- ◆ WebDAV jest protokołem dzielenia plików poprzez HTTP
 - alternatywa dla SMB zgodna z RFC 2518
 - wsparcie niektórych producentów oprogramowania
- ◆ IIS 5.0/6.0 obsługują WebDAV jako foldery web

EFS i WebDAV

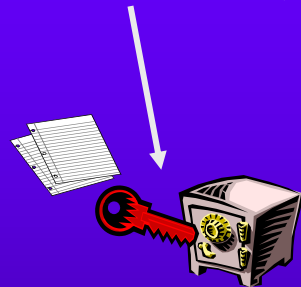
Klient łączy się z udziałem WebDAV



protokół HTTP

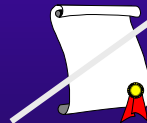


Server informuje klienta, że folder jest zaszyfrowany



Lokalna enkrypcja EFS

Plik w trybie RAW przesyłany do serwera





Rozszerzenia PKI

- ◆ Opcja auto-enrollment dla użytkowników
 - można skonfigurować dla certyfikatów EFS
 - automatyczne odnawianie certyfikatów
- ◆ Odtwarzanie kluczy
 - .NET CA umożliwia archiwizację kluczy prywatnych
 - tylko certyfikaty v2 mogą być odtworzone



Zalecenia dla .NET

- ◆ Pracuj w domenie!
- ◆ Wykorzystuj archiwizację kluczy poprzez .NET CA
- ◆ Współdzielenie plików powinno wykorzystywać Active Directory
- ◆ Nie należy używać 3DES w mieszanej domenie (chyba, że wszystkie pliki trzymane są na serwerze)



Tips and Tricks



Sprawdzanie użycia EFS

- ◆ Należy sprawdzić istnienie kluczy:
- ◆ Windows 2000
 - HKCU\Software\Microsoft\Windows NT\Current Version\EFS\CurrentKeys\CertificateHash
- ◆ Windows .NET
 - HKCU\Software\Microsoft\Windows NT\Current Version\EFS\CurrentKeys\CertificateHash
 - HKCU\Software\Microsoft\Windows NT\Current Version\EFS\CurrentKeys\Flag



Dodanie do menu kontekstowego

- ◆ W celu uruchomienia szyfrowania/deszyfrowania w menu kontekstowym należy ustawić klucz:
 - HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
 - Name: EncryptionContextMenu
 - Type: DWORD
 - Value: 1
- ◆ Należy zrestartować explorera



Uaktualnianie DRA

- ◆ Tylko w Windows .NET
- ◆ Zmienia pole DRF po zmianie DRA poprzez komendę „Cipher.exe /U”

A screenshot of a Windows command prompt window. The title bar reads "C:\WINDOWS\System32\cmd.exe". The command prompt shows the following text:

```
C:\Download>cipher /u  
C:\Download\readme.txt: Encryption updated.  
  
C:\Download>
```

The window has a standard Windows interface with minimize, maximize, and close buttons in the title bar, and a scroll bar on the right side.



Brak szyfrowania plików

- ◆ Pliki tymczasowe
- ◆ Pagefile
- ◆ Plik hibernacji
- ◆ Przy konwersji istniejących plików tekstowych
 - Tworzony jest plik tymczasowy
 - NTFS może nie zamazywać miejsca po starym pliku
 - Cipher /W w Windows .NET



Czyszczenie pagefile'a

- ◆ Należy sprawdzić czy pagefile jest czyszczony w trakcie wyłączenia systemu
- ◆ Ustawiane poprzez lokalną lub grupową politykę

Computer Configuration

Windows Settings

Security Settings

Local Policies

Security Options

Shutdown: Clear virtual memory pagefile



Stosowanie szyfrowania 3DES

- ◆ Tylko Windows .NET
- ◆ Zwiększa siłę enkrypcji w stosunku do domyślnej
- ◆ Ustawiane poprzez lokalne lub grupowe polityki

Computer Configuration

Windows Settings

Security Settings

Local Policies

Security Options

System Cryptography: Use FIPS compliant algorithms for encryption object



Więcej informacji

- ◆ Best Practices for EFS – Knowledge Base Article Q223316
- ◆ Using 3rd Party CAs for issuing EFS and EFS Recovery certificates - Knowledge Base Article Q273856
- ◆ EFS for Windows 2000 –
<http://www.microsoft.com/TechNet/win2000/win2ksrv/technote/nt5efs.asp>



Pytania ?

Sagus@hoga.pl