EFS Short Notes

DDF = Data Decryption Field
DRF = Data Recovery Field
DRA = Data Recovery Agent

****

CAPI = Crypto API 1.0
Standard fuer Verschluesselungs- und Signaturalgorithmen

****

SYSKEY = zusaetzlicher Schutz = Aktiv, kann auch zur Eingabe beim Systemstart fordern
Start – Ausfuehren – Syskey.exe

****

CSP = Cryprographic Service Provider
Stellt kryptografische Funktionen zur Verfuegung

****

Lokaler Administrator = DRA
Erster Administrator im Forest/Domain = DRA

****

Symmterische Verschlüsselung des Datenteils (Payload)
FEK = File Encryption Key)
FEK wird mit oeffentlichem RSA Schluessel des Benutzers verschluesselt
Die geheimen Schluessel werden in C:\Dokumente und Einstellungen\<User>\Anwendungsdaten\Microsoft\Crypto\RSA\ des Benutzerprofils gespeichert und mit dem Master Key des Users chiffriert.

Asymmetrische Verschluesselung des Verschluesselungs-Schluessels

RSA Private Key wird mit einem Hash des NTLM Kennworts und des Benutzernamen verschluesselt

Sicherung bei XP = 64 Bit 3DES

Master Key wird alle 60 Tage erneuert

XP ab SP1 = Default AES 256 Bit

FEK wird im $EFS alternativen Daten Stream (ADS) der Datei "versteckt"

****

EFS und WebDAV
- Verteilter Zugriff auf verschluesselte Dateien
- Ab Windows Server 2003
- Maximal 400 MB
- Verzeichnis mit WebDAV "sharen"
- Verschluesselung nur ueber WebDAV
- Administrator sieht lokal unverschluesselte Dateien

****

Remote Encyrption
- Benutzer einer Arbeitsstation kann Dateien Remote verschluesseln
- Deaktivieren der Funktion "sensitive and cannot be delegated" fuer den Account
- Computer muss "Trusted for Delegation" sein

****

EFS File Sharing mit XP
- EFS Zertifikat fuer User anfordern
- Benutzerzertifikat zur verschluesselten Datei hinzufuegen

****

Ordner werden nicht verschluesselt, nur Dateien

****

EFS deaktivieren per lokaler oder DOmaenen GPO

****

Autoenrollment von EFS Zertifikaten ist moeglich
- Basis EFS Template sollte deaktiviert werden
- Neues Template mit Schluesselarchivierung und
- Superseeded Template fuer Basis EFS Template

****

CIPHER
- Command Line Tool
- /K = Neuer FEK
- /X = Backup PFX

****

EFS in Arbeitsgruppe
- Password Reset Disc fuer lokale XP und Windows 2003 Server ohne Domaene

****

PKI - Schluesselarchvirung
- Schluesselarchivierungs Agenten einrichten
- CA fuer Schluessel Archivierung aktivieren
- Template mit Schluessel Archivierung erstellen

****

Gruppenrichtlinien
- EFS aktiv JA/NEIN
- DRA hinzufuegen
- DRA erstellen

****

EFS auf Smartcard
- Ab Vista

****

Autoenrollment von EFS Zertifikaten
- Neues Template in Enterprise CA erstellen
- Autoenroll Berechtigungen setzen
- Autoenrollment in GPO aktivieren

****

Keine CA vorhanden = Self signed EFS Zertifikat

****

Best Practice
- Enterprise CA installieren
- Schluesselarchivierung aktivieren
- EFS Template mit Schluesselarchivierung
- Superseeding Basic EFS Template
- Autoenrollment konfigurieren
- EFS Wiederherstellungsagenten hinzufuegen
- EFS Wiederherstellungszertifikat sichern

****

EFS Erweiterungen in Windows Vista und Windows Server 2008 (Source: Wikipedia.de - http://de.wikipedia.org/wiki/Encrypting_File_System)

Per-user encryption of Client-Side Cache (offline files) support for storing (user or DRA) RSA private keys on A PC/SC smart card
EFS Re-Key Wizard
EFS Key backup prompts
Support for deriving DPAPI Master Key from PC/SC smart card

Support for encryption of pagefile.sys
Protection of EFS-related secrets using BitLocker (Enterprise or Ultimate edition of Windows Vista)
Group Policy controls to enforce:
- encryption of Documents folder
- offline files encryption
- indexing of encrypted files
- requiring smart card for EFS
- creating a caching-capable user key from smart card
- displaying a key backup notification when a user key is created or changed
- specifying the certificate template used for enrolling EFS certificates automatically