Sedí dva velmi smutní informatici v serverové místnosti.
Přijde k nim třetí a ptá se: "A cože jste tak smutní?"
"No, včera jsme se trošku ožrali a měnili jsme hesla...

Podzim 2008

PV175 SPRÁVA MS WINDOWS I

Šifrování
Boot možnosti

Šifrování

- EFS (Encrypting File System)
  - Transparentní šifrování souborů na systémech XP Professional, Vista Business a vyšší
  - Zajištění důvěrnosti ukládaných dat i v případě, kdy systém neběží (na rozdíl od řízení přístupu)
  - Data jsou šifrována symetrickým klíčem, který samotný je zašifrován veřejným klíčem spojeným s certifikátem uživatele
    - Klíč symetrické kryptografie je odlišný pro každý soubor (FEK = File Encryption Key)
    - Privátní klíč je odvozen z uživatelského jména a hesla
      - Změna hesla zneplatňuje klíč (!!!) – existuje hotfix

Omezení EFS

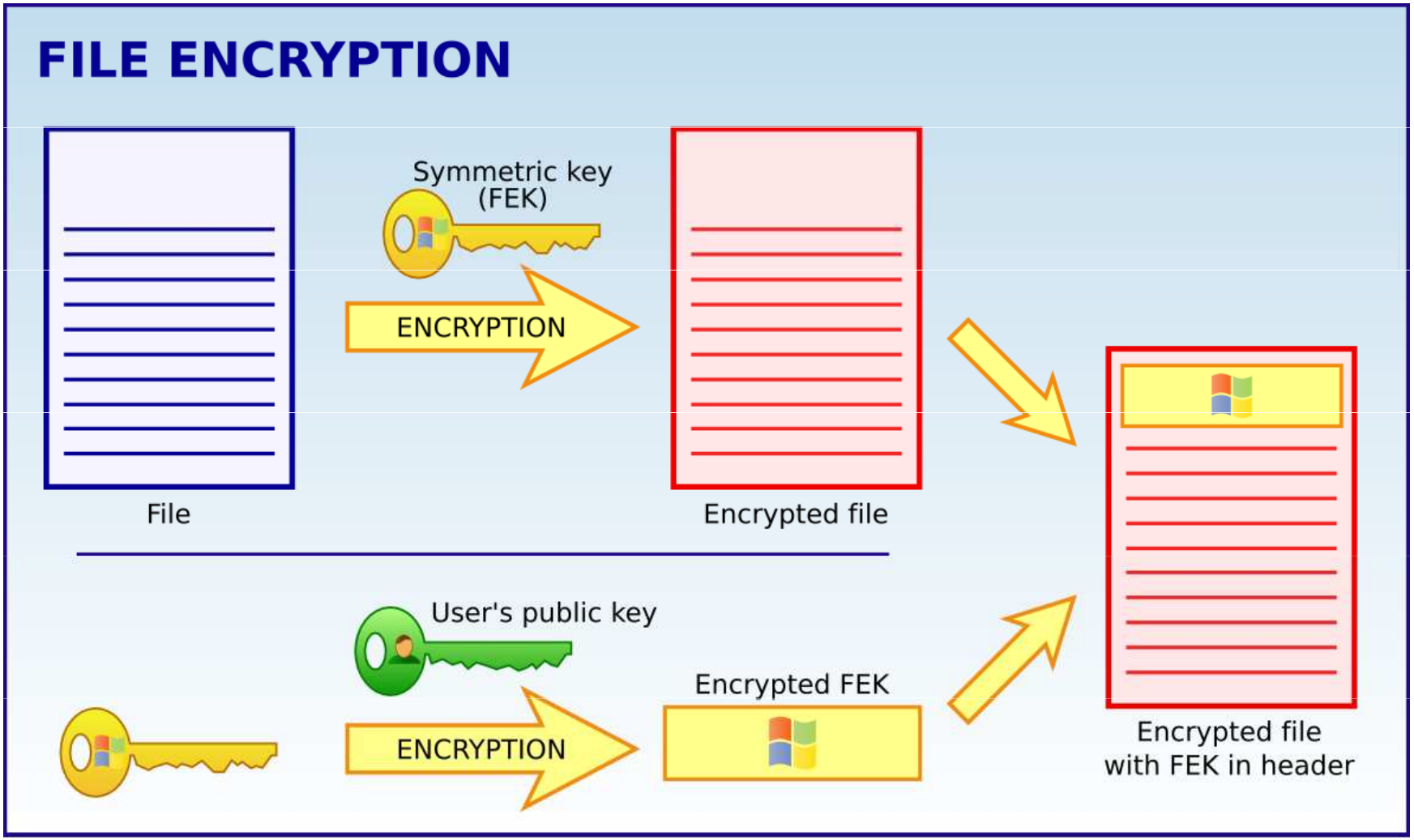
- Použitelné pouze na NTFS (v případě přenosu souboru oprávněným uživatelem na jiný souborový systém je soubor automaticky dešifrován, stejně tak při přenosu po síti)
- Nelze využít spolu s kompresí
- Některé soubory není možné šifrovat (např. obsah složky %systemroot%)
- EFS je možné zakázat na úrovni souboru, složky i počítače
- EFS není použitelné pro soubory v cestovních profilech

Použití EFS

1. Nastavení atributu šifrování souboru nebo složky (hodnota atributu na složce se dědí do vnořených souborů složek). Pokud dosud neexistuje uživatelský certifikát, pak je automaticky vytvořen.
2. Ověření, zda uživatel vlastní klíč pro dešifrování souboru (viz dále).
3. Pokud ano, je mu soubor okamžitě zpřístupněn v otevřené podobě, jinak je mu přístup znemožněn.

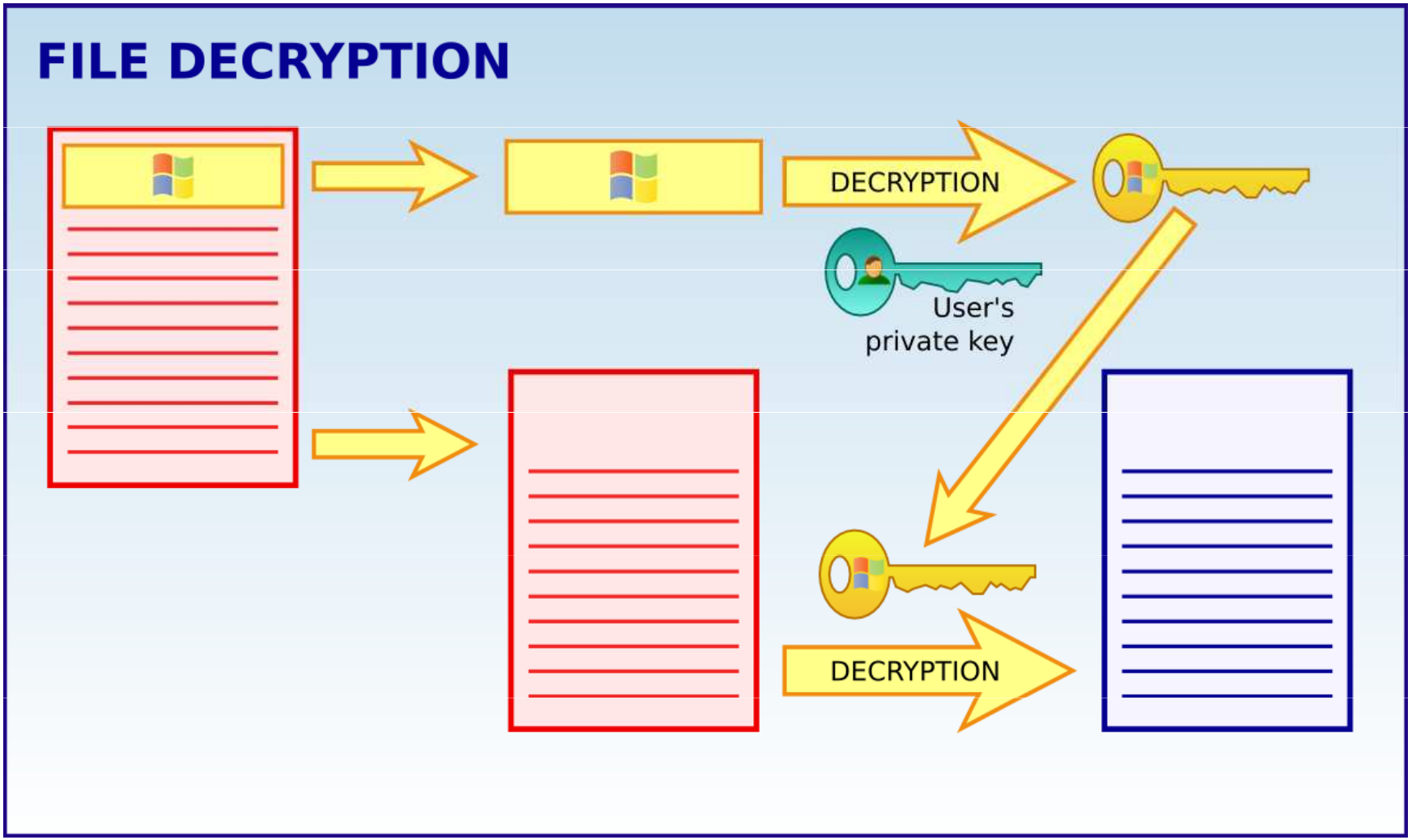
Šifruje se certifikátem, ne uživatelem!
Změna nebo zavedení nového certifikátu odebírá přístup k souborům zašifrovaným starým certifikátem.

EFS šifrování



(wikipedia.org)

EFS dešifrování

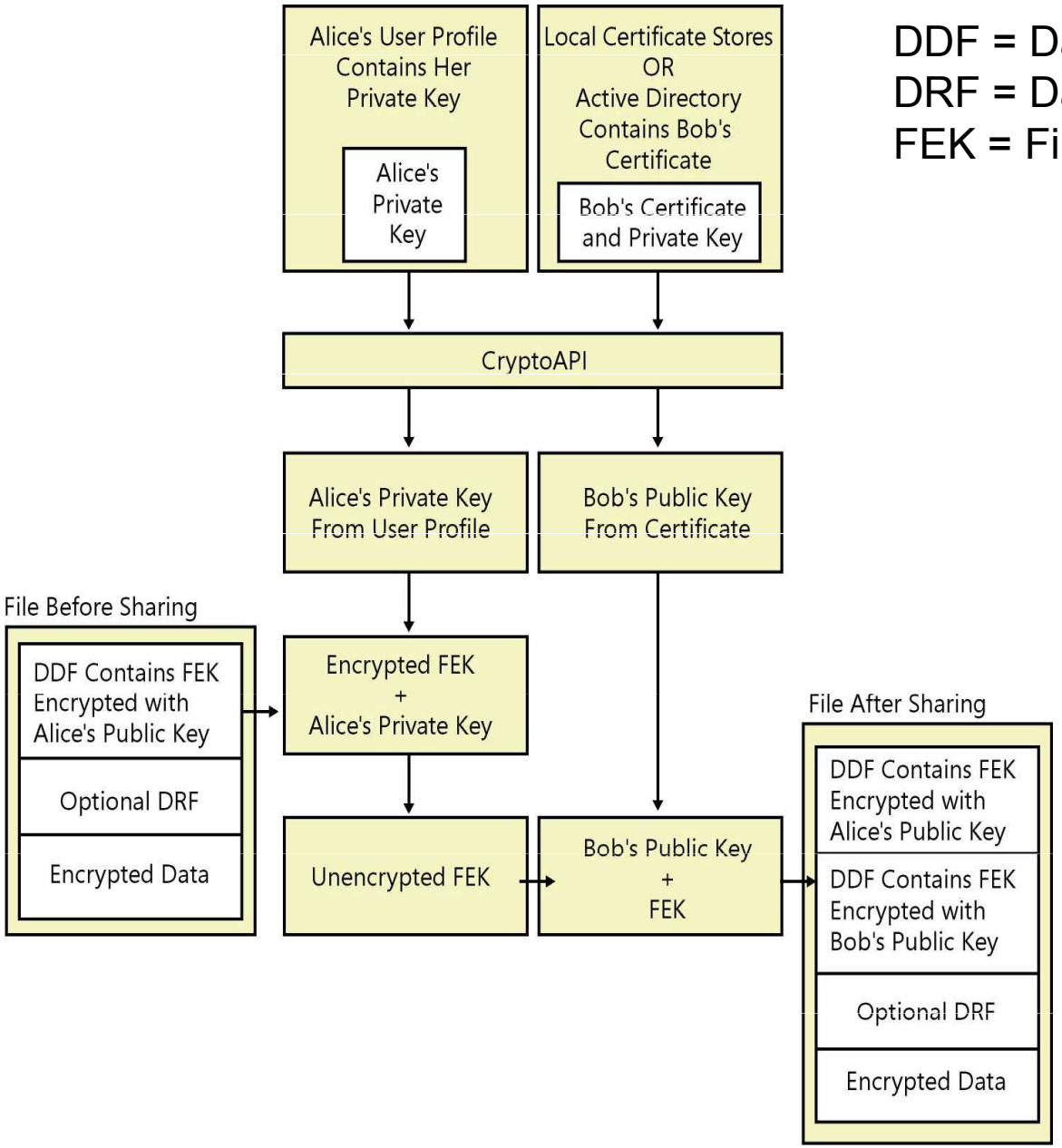


(wikipedia.org)

Recovery agent

- K šifrovanému souboru může přistupovat souběžně více uživatelů (sdílení šifrovaných souborů)
- Obvykle je vhodné toto sdílení vynutit (možnost záchrany dat i v případě zapomenutí hesla nebo odchodu zaměstnance) – zde přichází na řadu agenti obnovení (recovery agents)
  - Gpedit.msc: Computer Settings – Windows Settings – Security Settings – Public Key Policies – Encrypting File System – Add Data Recovery Agent
  - Vytvoření certifikátu agenta obnovení: cipher /r:path
  - Agenti obnovení mohou obnovit pouze soubory vytvořené nebo modifikované po jejich přiřazení do GPO

Sdílení a agenti obnovení



DDF = Data Decryption Field
DRF = Data Recovery Field
FEK = File Encryption Key

Obnova po chybě

- Minimem je mít aspoň 2 certifikáty schopné dešifrovat každý soubor – ochrana před poškozením certifikátu
  - Využití Recovery agenta (často vyžadováno vnitřními nařízeními organizace)
  - Případně záložní uživatelský účet
- Zálohovat použité certifikáty – ochrana před pádem celého systému
  - certmgr.msc – Personal – Certificates – Export
  - Zahrnout zálohování certifikátů do pravidelných záloh souborů

EFS Best practices

- Šifrovat složky a ne přímo soubory, nezapomínat na šifrování Temp složek
- Vytvořit ideálně několik Recovery agentů, kteří nebudou používáni pro nic jiného než dešifrování v případě nouze
- Exportovat z počítače certifikát a privátní klíč uživatelského účtu, který funguje jako Recovery agent, ochránit ho silným heslem a uložit na externí úložiště
  - Recovery agent nadále není schopen prohlížet šifrované soubory, takže jeho kompromitace nenaruší důvěrnost dat.
- Použít 3DES šifrovací algoritmus
- Použít silné heslo uživatelského účtu

BitLocker

- Šifrování celých partition ve Windows Vista Enterprise a Ultimate
  - Nejsou přístupné ani organizační údaje o datech na disku
- AES šifrovací algoritmus, 128b délka klíče
- Podporuje i USB mód
  - Zavedení operačního systému je možné pouze v případě, kdy uživatel disponuje USB klíčem s příslušnými daty.
- Neochraňuje před přístupem v rámci systému (vícero uživatelů nebo procesů) – vzájemná spolupráce s EFS

Možnosti startu systému

- F8 při startu Windows
- Safe mode
  - Načteny jen základní ovladače a systémové služby, nenačítá služby pro připojení k síti
  - Ignoruje lokální politiky, uživatelský profil, programy po spuštění
  - Načítá pouze generický ovladač grafiky vga.sys
- Safe mode with networking
  - Načteny navíc služby sítě, aplikovány politiky
- Safe mode with command prompt
  - Nenačte se grafické rozhraní

Možnosti startu systému II

- Poslední známá konfigurace (Last known good configuration)
  - Pomůže, pokud nově nainstalovaný ovladač brání startu systému.
  - Umožní naběhnutí systému i pokud byl zakázán ovladač nutný pro úspěšný boot.
- Zapnout režim VGA
  - Spuštění Windows s rozlišením 640x480 při použití aktuálního grafického ovladače.

Recovery console

- Vstup přes instalační médium
- Umožňuje omezený přístup k diskům se souborovým systémem NTFS, FAT, FAT32 i bez spuštění grafického rozhraní
- Akce
  - Používat, kopírovat, přejmenovat nebo nahradit systémové soubory a složky
  - Povolit / zakázat spuštění služby nebo driveru při startu
  - Opravit zaváděcí sektor systému souborů nebo hlavní spouštěcí záznam (MBR)
  - Spravovat a formátovat oddíly jednotek

Dotazy?

Díky za pozornost