MS Windows 2000 Encrypting File System

Gliederung

- Prolog
- Funktionen der Dateiverschlüsselung
- EFS-Features
- Dateien und Verzeichnisse verschlüsseln
- Persönliche Zertifikate verwalten
- Verschlüsselte Dateien wiederherstellen
- Wiederherstellungszertifikate verwalten
- Wiederherstellungsagenten hinzufügen
- Dateien auf Dateiservern verschlüsseln

Prolog
Begriffsfindung

- Begriffsfindung gemäß dem

  Gesetz zur Regelung der Rahmen-bedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz - IuKDG)

  vom 22. Juli 1997 (Bundesgesetzblatt - BGBl. I S.1870)

Prolog
IuKDG, digitale Signatur

- Gesetz zur digitalen Signatur (Signaturgesetz - SigG) gemäß IuKDG, Artikel 3, §2, Absatz (1)

  Eine digitale Signatur im Sinne dieses Gesetzes ist ein mit einem privaten Signaturschlüssel erzeugtes Siegel zu digitalen Daten, das mit Hilfe eines zugehörigen öffentlichen Schlüssels, der mit einem Signaturschlüssel-Zertifikat einer Zertifizierungsstelle oder der Behörde nach § 3 versehen ist, den Inhaber des Signaturschlüssels und die Unverfälschtheit der Daten erkennen läßt.

Prolog
Digitale Signatur

- Wozu eine digitale Signatur?
  - Authentität (die Herkunft der Daten muss nachweisbar sein),
  - Integrität (die ausgetauschten Daten haben nur Gültigkeit wenn der Inhalt sowie die angeführten Adressen unversehrt sind),
  - Vertraulichkeit (die Daten sind vor der Einsicht durch Unbefugte geschützt),
  - Verbindlichkeit (der Absender kann nicht leugnen die Nachricht selbst versendet zu haben).

Prolog
IuKDG, Zertifizierungsstelle

- Gesetz zur digitalen Signatur (Signaturgesetz - SigG) gemäß IuKDG, Artikel 3, §2, Absatz (2)

  Eine Zertifizierungsstelle im Sinne dieses Gesetzes ist eine natürliche oder juristische Person, die die Zuordnung von öffentlichen Signaturschlüsseln zu natürlichen Personen bescheinigt und dafür eine Genehmigung gemäß § 4 besitzt.

Prolog
IuKDG, Zertifikat

- Gesetz zur digitalen Signatur (Signaturgesetz - SigG) gemäß IuKDG, Artikel 3, §2, Absatz (3)

  Ein Zertifikat im Sinne dieses Gesetzes ist eine mit einer digitalen Signatur versehene digitale Bescheinigung über die Zuordnung eines öffentlichen Signaturschlüssels zu einer natürlichen Person (Signaturschlüssel-Zertifikat) oder eine gesonderte digitale Bescheinigung, die unter eindeutiger Bezugnahme auf ein Signaturschlüssel-Zertifikat weitere Angaben enthält (Attribut-Zertifikat).

Prolog
IuKDG, Zertifikatsinhalt

- Gesetz zur digitalen Signatur (Signaturgesetz - SigG) gemäß IuKDG, Artikel 3, §7, Absatz (1)

  Das Signaturschlüssel-Zertifikat muß folgende Angaben enthalten:

  – den Namen des Signaturschlüssel-Inhabers, der im Falle einer Verwechslungsmöglichkeit mit einem Zusatz zu versehen ist, oder ein dem Signaturschlüssel-Inhaber zugeordnetes unverwechselbares Pseudonym, das als solches kenntlich sein muß,

Prolog
IuKDG , Zertifikatsinhalt

Fortsetzung (1) IuKDG, Artikel 3, §7, Absatz (1):

- den zugeordneten öffentlichen Signaturschlüssel,
- die Bezeichnung der Algorithmen, mit denen der öffentliche Schlüssel des Signaturschlüssel-Inhabers sowie der öffentliche Schlüssel der Zertifizierungsstelle benutzt werden kann,
- die laufende Nummer des Zertifikates,
- Beginn und Ende der Gültigkeit des Zertifikates,

Prolog
IuKDG , Zertifikatsinhalt

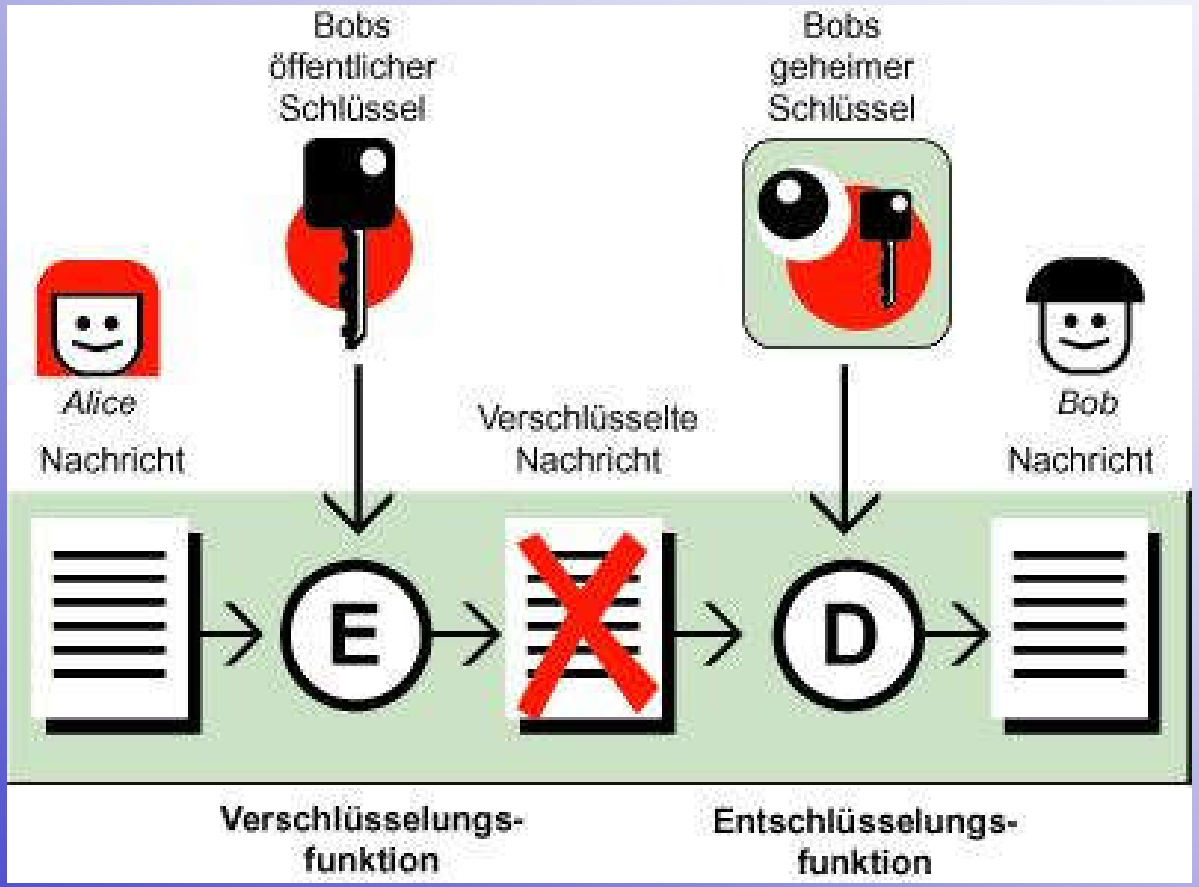
Fortsetzung (2) IuKDG, Artikel 3, §7, Absatz (1):

- den Namen der Zertifizierungsstelle und
- Angaben, ob die Nutzung des Signaturschlüssels auf bestimmte Anwendungen nach Art und Umfang beschränkt ist.

Prolog
Zertifikatsaufbau nach X.509

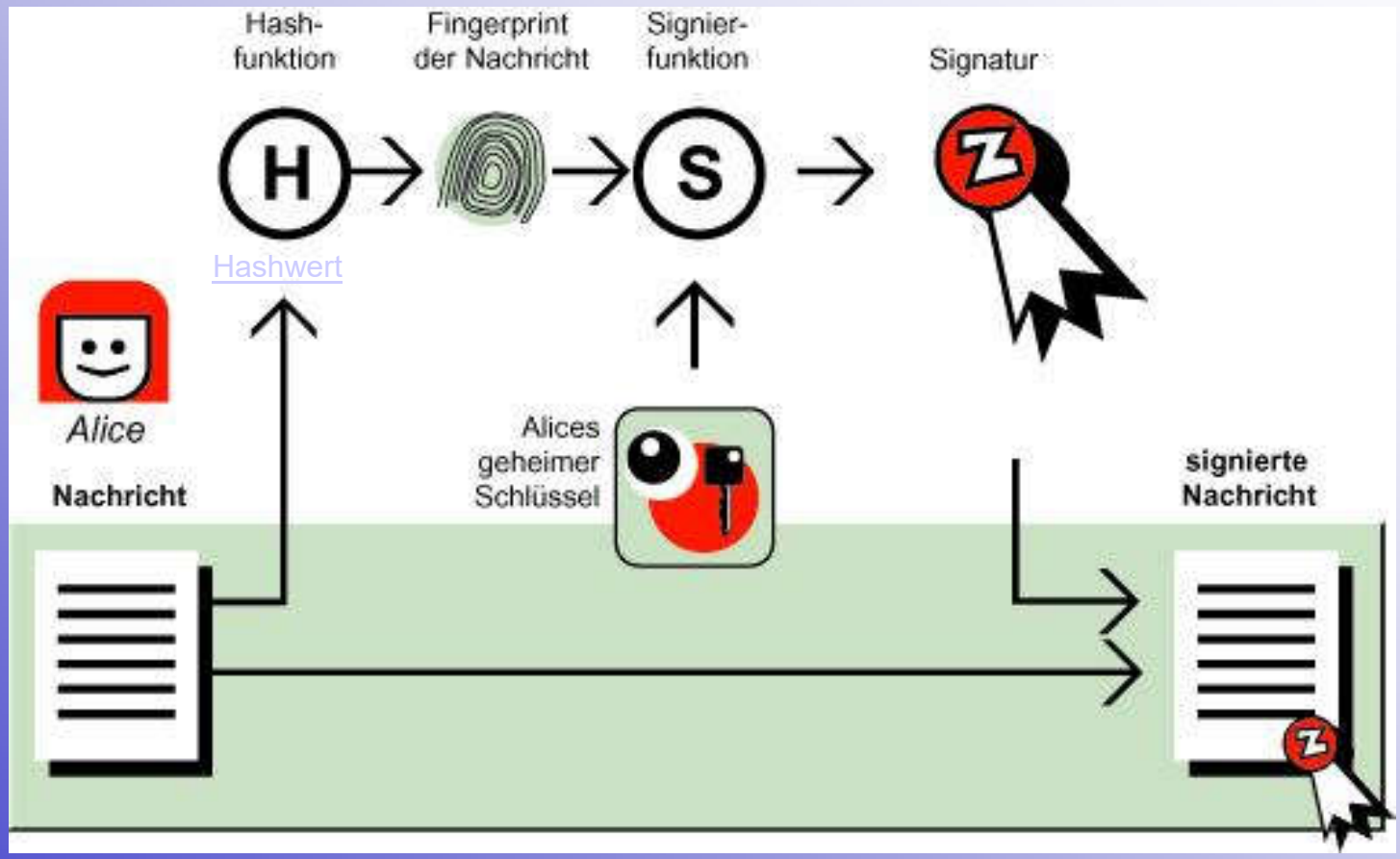
Version [Zertifikatsformat]
Seriennummer [von Trust Center vergeben]
Signatur-Algorithmus
Aussteller
Gültigkeitsintervall • **nicht vor Datum** • **nicht nach Datum**
Entitätsname [zugeordneter Besitzer]
Öffentlicher Schlüssel der Entität • **Verwendeter Algorithmus** • **Öffentlicher Schlüssel**
Erweiterungen [wofür verwendbar, OID]
Signatur des Trust Center

Prolog
Zwei-Schlüssel-Verfahren (asym.)

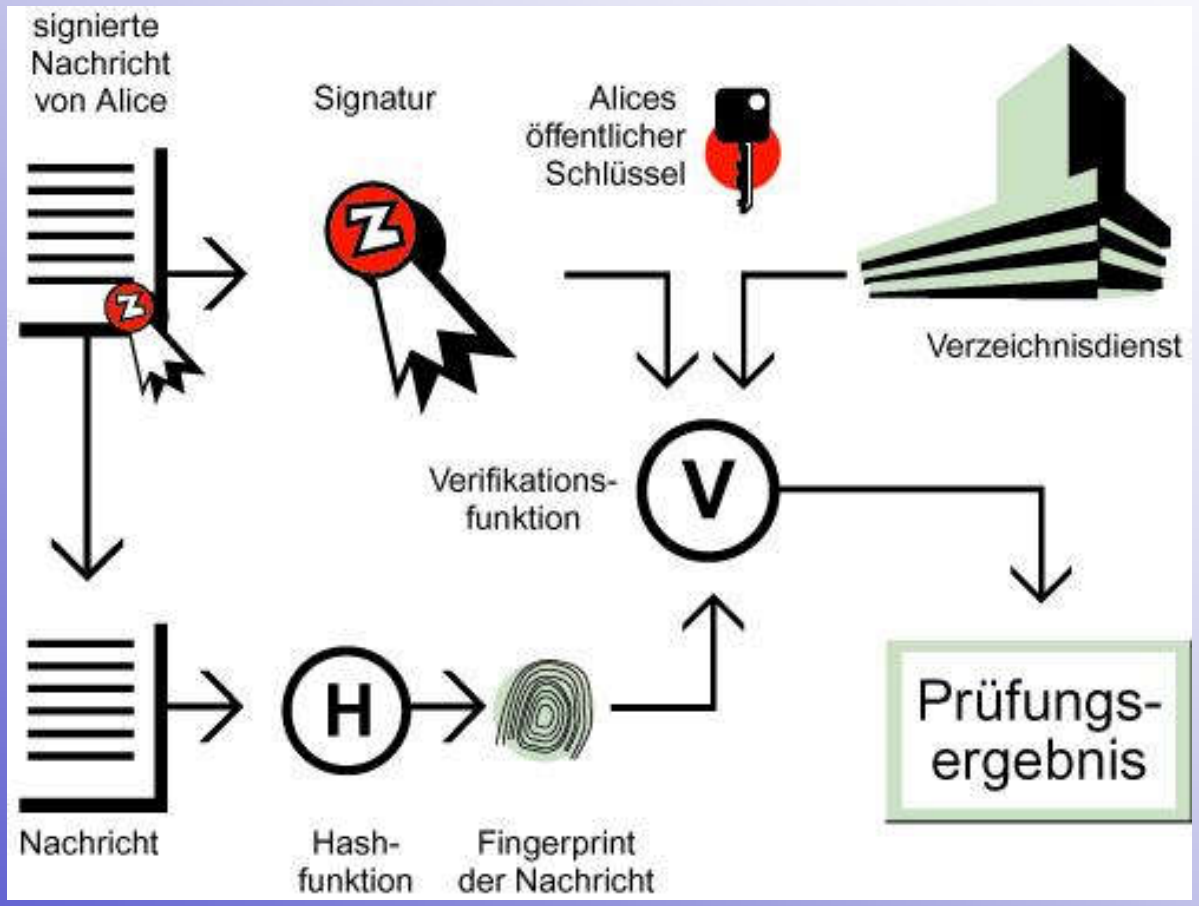


Anmerkung:
Die klassischen Namen für Sender und Empfänger bei Beispielen mit kryptografischem Hintergrund sind „Alice“ und „Bob“!

Prolog
Signatur



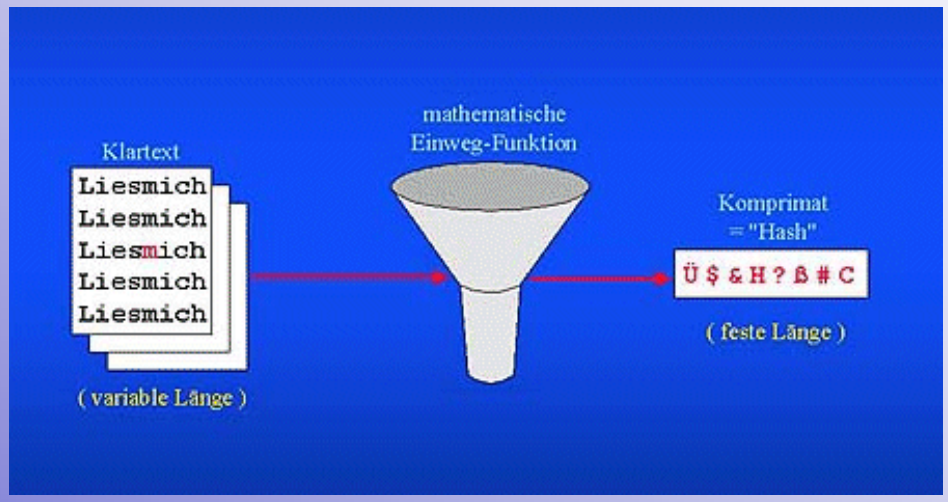
Prolog
Signatur verifizieren



Prolog

Die Hashfunktion

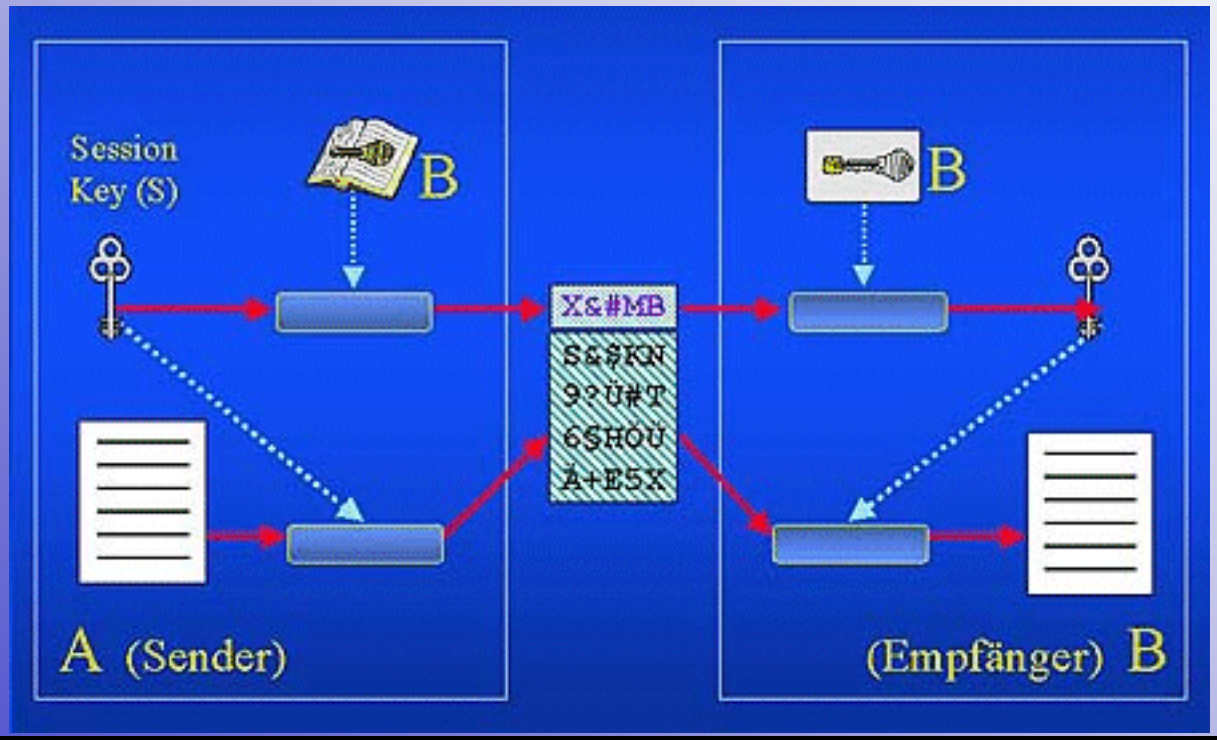
- Eine Hashfunktion ist eine Rechenvorschrift, die aus einem beliebigen Eingabetext eine Ausgabe mit stets fester Länge erzeugt (Einwegfunktion).
- Unterschiedliche Eingaben liefern immer unterschiedliche Ausgaben!



Online Hash-Berechnung Zurück zur Signatur

Prolog
Gängige Verschlüsselungstechniken

- Standardverfahren ist die Hybridverschlüsselung, da sicher (asymmetrisch) und schnell (symmetrisch)



Prolog
symmetrisch vs. asymmetrisch

- Vergleich der Schlüssellängen bei angenommener identischer Sicherheitsstufe:

Symmetr. Schlüssellänge	Asymmetr. Schlüssellänge
56 Bit	384 Bit
64 Bit	512 Bit
80 Bit	768 Bit
112 Bit	1792 Bit
128 Bit	2304 Bit

- Asymmetrische Rechenverfahren sind, verglichen mit symmetrischen Verfahren, ca. um den Faktor 100 bis 1000 langsamer.
- Eine RSA-Brute-Force-Attack bei 512 Bit Schlüssel-länge dauert ca. 8000 MIPS-Jahre

Prolog
Zusammenfassung

- Zusammenfassung I
  - *Digitale Signatur:* Asymmetrische Verschlüsselung eines Dokuments oder dessen Hashwert mit dem Privatschlüssel des Absenders zur Identifikation desselben.
  - *Zertifikat:* Mit dem Privatschlüssel eines Trust Centers verschlüsselte Daten (Identität, öffentl. Schlüssel u. a.) zur Beglaubigung eines Objekts (Benutzer, Website o. ä., auch „Entität“ genannt).
  - *Trust Center* (auch CA=Certification Authority genannt) sind Zertifizierungsstellen, die sich durch Stammzertifizierungsstellen (Root-CA) zertifizieren, letztere zertifizieren sich gegenseitig oder selbst.

Prolog
Zusammenfassung

- Zusammenfassung II
  - *Asymmetrische Kryptographie:* Verschlüsselung auf Basis eines öffentlichen und privaten Schlüssels: rechenaufwendige Algorithmen, öffentlicher Schlüssel darf allen bekannt sein.
  - *Symmetrische Kryptographie:* Verschlüsselung auf Basis eines Schlüssels: schnelle Algorithmen, der Schlüssel darf jedoch nicht an die Öffentlichkeit gelangen.
  - *Hybride Verschlüsselung:* Datenübermittlung unter Verwendung eines schnellen symmetrischen Verschlüsselungsverfahrens, dessen Schlüssel (Session-Key) vorher mit Hilfe des asymmetrischen Zwei-Schlüssel-Verfahrens dem Kommunikationspartner chiffriert übermittelt worden ist.

Prolog
Anwendungsgebiete

- Mögliche Einsatzgebiete
  - Aktuell: Sicherung des Border Gateway Protocol (BGP) bei Routerkommunikation ==> S-BGP, siehe auch: http://www.internetweek.com/story/INW20011217S0004,
  - Online Banking,
  - Übertragung von Personendaten und Kreditkarten- oder Kontonummern beim eCommerce,
  - Softwareupdates oder Browser-Plug-In Installation via Internet,
  - Echtheitsbestätigung bei und Sicherung von E-Mails,
  - Verschleierung von Viren gegenüber Virenscannern,
  - Dateiverschlüsselung/EFS ;-).

Gliederung

- Prolog
- Funktionen der EFS-Dateiverschlüsselung
- EFS-Features
- Dateien und Verzeichnisse verschlüsseln
- Persönliche Zertifikate verwalten
- Verschlüsselte Dateien wiederherstellen
- Wiederherstellungszertifikate verwalten
- Wiederherstellungsagenten hinzufügen
- Dateien auf Dateiservern verschlüsseln

EFS-Dateiverschlüsselung
EFS-Grundlagen

- Warum Verschlüsselung?
- Wie wird verschlüsselt?
  - Zentraler Encrypting File System Treiber: EFS.SYS,
  - Benutzung des DESX (Extended US Data Encryption Standard):
    - 64-Bit-Block XOR Verschlüsselungs-Algorithmus,
    - DES Verschlüsselung mit 56-Bit-Schlüssel,
    - 64-Bit-Block XOR Verschlüsselungs-Algorithmus,
    - Besserer (?) Schutz vor Brute Force Angriffen als Standard-DES (laut Microsoft),
  - Symmetrisches Verfahren,
  - Schnell bzgl. Ver-/Entschlüsselung,
  - Schutz des symm. Schlüssels (hybride Verschlüsselung).

EFS-Dateiverschlüsselung
DES-Grundlagen

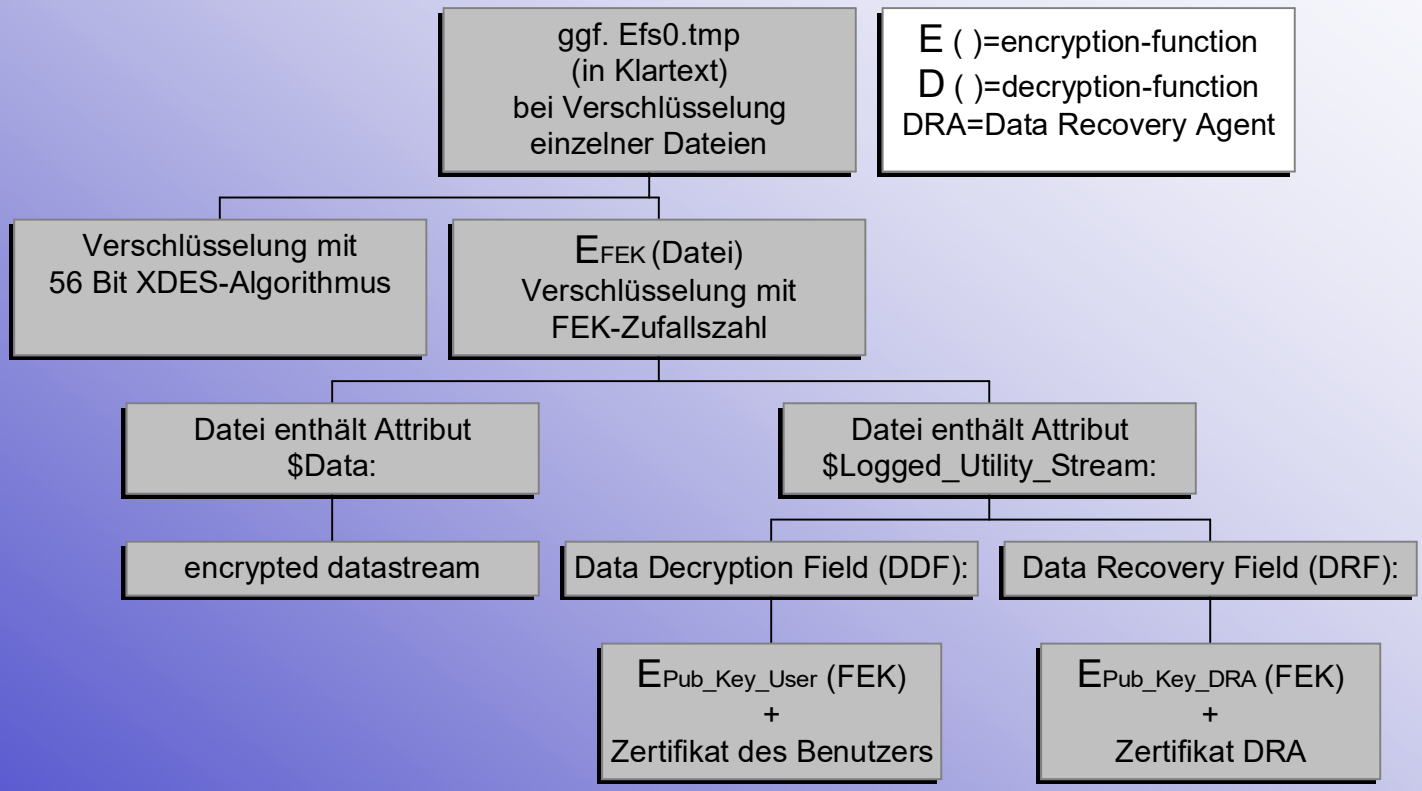
- Standard-DES (schnell, standardisiert, alt, unsicher)
  - Nach einer Eingangspermutation wird ein 64 Bit Block in eine jeweils 32 Bit lange rechte und linke Hälfte zerlegt. Jetzt folgen 16 Runden identischer Operationen - die sogenannte Funktion f - in denen die Blöcke mit dem Schlüssel und unter-einander kombiniert werden und anschließend vertauscht werden. Nach der sechzehnten Runde werden rechte und linke Hälfte zusammengefügt. Eine Schlußpermutation, die zur Eingangspermutation invers ist, schließt den Algorithmus ab. □

EFS-Dateiverschlüsselung
Der File Encryption Key

- Der File Encryption Key (FEK)
  - Standard: 56-Bit FEK-Zufallszahl, optional: 128-Bit
- Schutz des FEK
  - Verschlüsselung mit der Technologie des langsamen aber sehr sicheren Public Key Cryptography System (PKCS)
  - PKCS ist ein asymmetrisches Verfahren mit einem öffentlichen und einem privaten Schlüsselpaar
  - Privater Schlüssel wird mit MD4-Hash des Benutzerkenn-worts verschlüsselt (XDES-Algorithmus??)
  - MD4-Verfahren enthält kryptogr. Schwächen lt. RSA Data Security

EFS-Dateiverschlüsselung
Aufbau Dateiverschlüsselung

EFS-Verschlüsselung einer Datei



EFS-Dateiverschlüsselung
EFS-Dateien öffnen

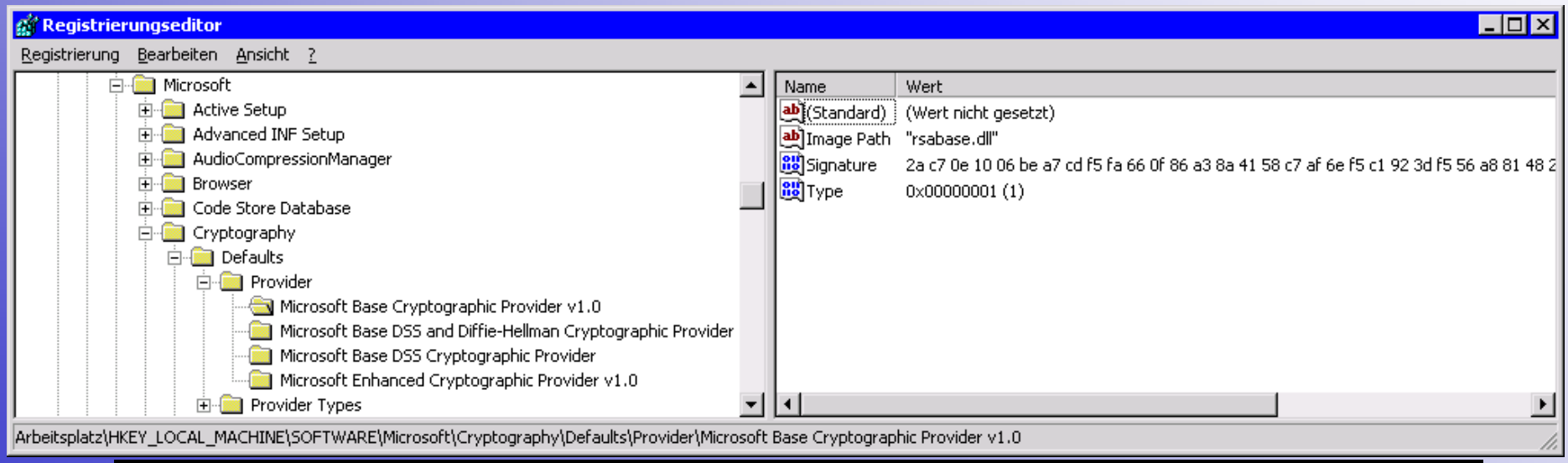
- Öffnen einer verschlüsselten Datei:
  - EFS liest Zertifikat aus dem *$Logged_Utility_Stream*-Attribut (DDF) aus
  - EFS fordert mit Benutzer-Zugriffstoken bei LSA (Local Security Authority) den Privat-Key an, dessen Besitzer über das Zertifikat verifiziert wird
  - EFS erzeugt den FEK durch

    $D_{Priv\_Key\_User}(E_{Pub\_Key\_User}(FEK))$
  - EFS erzeugt unverschlüsselten Datenstrom durch

    $D_{FEK}(E_{FEK}(\$Data))$
  - EFS sendet nun diesen unverschlüsselten Datenstrom an die anfordernde Anwendung

EFS-Dateiverschlüsselung
Kryptographie-Anbieter

- Schlüssel erzeugen
  - jeder Win2K-Rechner ist grundsätzlich in der Lage, EFS-Schlüssel auszustellen
  - LSA erstellt bei Bedarf Benutzer-Schlüsselpaar mithilfe des Kryptografiediensteanbieter



EFS-Dateiverschlüsselung
Registry-Einträge

- Schlüsselablage
  - Private Key (proprietäres Format, mit gehashtem Benutzerpaßwort verschlüsselt) in:

    \Dokumente und Einstellungen\Username\ Anwendungsdaten\Microsoft\Crypto\User_SID

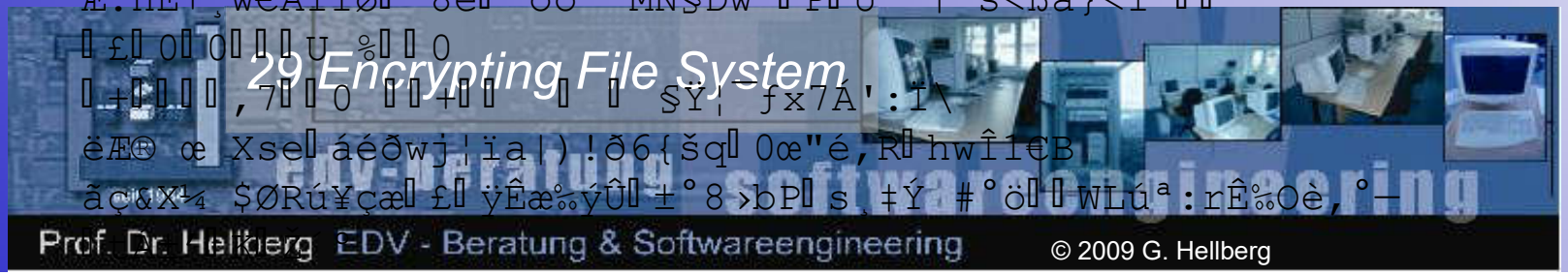
    (Achtung bei Kontenwechsel oder Wechsel von lokalem Useraccount zu Domänenaccount!)
  - Public Key-Zertifikat in:

    \Dokumente und Einstellungen\Username\ Anwendungsdaten\Microsoft\SystemCertificates\ My\Certificates
  - EFS-Zertifikate auch verwaltbar durch CAs

EFS-Dateiverschlüsselung
Public-Key-Zertifikat als Datei

- Dateiname (=Zertifikats-Fingerprint / Hash):
  048D56636BE9AFD413827562BDB4577B507B5204

```
    □   Ä       l   □                   □   5 e b 3 1 b 6 d -
e b 7 b - 4 d 3 9 - a 7 b 9 - a 0 c 1 a a d 1 2 4 e a
M i c r o s o f t   B a s e   C r y p t o g r a p h i c
P r o v i d e r   v 1 . 0     □   □   □
□Vcké¯Ô□,ub½´W{P{R□     □    ,
0, (0,□ □ □  □¾Û×□¡Ùx™M½'sUähó0    □□+□□  □ 0H1□0
□□U□□□□admin1
0□□U□ □□EFS1(0&□□U□
□ EFS File Encryption Certificate0 □011211162804Z□□
210111171628042Z0H1 □0
□□U□□□□admin1
0□□U□ □□EFS1(0&□□U□ EFS File Encryption Certificate0Ÿ0□
     *†H†÷□□□□ □ 0‰ □°ªE¶□—□"Ò¸-□¬Éç□}®ím. šæÕ □¡e□¹QòÑ·š
{ÖyÞŒHoûðpðƒ□ %:,ýBâ8□□9>6uÄZ□ .}úÇjç0âT2ácÎ—
Æ.HE+¸w€ÃÍÌø□`8e□"óò— MN$Dw`□P□Ù´ |`s<ßâ}<I □□
□£□0□0□□□U‰□□0
□+□□□□,7□□0 □□+□□  □ □ SŸ¦ ƒx7Á':Ì\
ëÆ® œ Xse□áéðwj¦ïa|)!ð6{šq□0œ"é,R□hwÎî€B□
ãç&X¼ $ØRú¥çæ□£□ÿÊæ‰ýÛ□±°8›bP□s¸‡Ý #°ö□□WLúª:rÊ‰Oè,°—
```



EFS-Dateiverschlüsselung
Der Data Recovery Agent

- Die Standard-Identität des Datenwieder-herstellungs-Agenten ist wie folgt festgelegt:
  - Win 2K Pro (auch innerhalb einer Domäne): lokales Konto des Administrator
  - Eigenständiger Win 2K Server: lokales Konto des Administrator
  - Win 2K DC oder Mitgliedsserver: AD-Konto Administrator

Gliederung

- Prolog
- Funktionen der Dateiverschlüsselung
- EFS-Features
- Dateien und Verzeichnisse verschlüsseln
- Persönliche Zertifikate verwalten
- Verschlüsselte Dateien wiederherstellen
- Wiederherstellungszertifikate verwalten
- Wiederherstellungsagenten hinzufügen
- Dateien auf Dateiservern verschlüsseln

EFS-Features
Basiswissen

- „Verschlüsselt“ ist ein eigenständiges Attribut (löschen/umbenennen trotzdem möglich)
- Dateisystem muss NTFS v5 sein
- Kopien temporärer Kopien sind nicht ver-schlüsselt (ausser in verschl. Verzeichnisse)
- Inhalte der Auslagerungsdatei sind verschlüsselt (?)
- In verschlüsselten Ordnern können andere Personen (unverschlüsselt) Dateien speichern

EFS-Features
Basiswissen

- Benutzerzertifikate sind im Profil gespeichert: lokale Profile NICHT löschen!
- Komprimierung und Verschlüsselung schließen sich gegenseitig aus
- Systemdateien sind nicht verschlüsselbar
- Freigabe verschlüsselter Dateien nicht möglich ==> Workaround: API-Aufruf *AddUsersToEncryptedFile()* nutzen

Gliederung

- Prolog
- Funktionen der Dateiverschlüsselung
- EFS-Features
- Dateien und Verzeichnisse verschlüsseln
- Persönliche Zertifikate verwalten
- Verschlüsselte Dateien wiederherstellen
- Wiederherstellungszertifikate verwalten
- Wiederherstellungsagenten hinzufügen
- Dateien auf Dateiservern verschlüsseln

Verschlüsselung Dat. & Verz.
Programme & Beispiele

- Konsole: Kommandozeilentool *CIPHER*
- GUI: Datei- oder Verzeichniseigenschaften - (Datei-) Attribute - Erweitert
- Praktische Demonstration:
  - *Arbeiten mit CIPHER*
  - *Verschlüsselung unter GUI*
  - *Eintragungen im Benutzerprofil*
  - *Befehl „Ver-/Entschlüsseln“ im Kontextmenü erzeugen*

Gliederung

- Prolog
- Funktionen der Dateiverschlüsselung
- EFS-Features
- Dateien und Verzeichnisse verschlüsseln
- Persönliche Zertifikate verwalten
- Verschlüsselte Dateien wiederherstellen
- Wiederherstellungszertifikate verwalten
- Wiederherstellungsagenten hinzufügen
- Dateien auf Dateiservern verschlüsseln

Persönliche Zertifikate
Einleitung

- Beim ersten Aufruf der Dateiverschlüsselung erzeugt das lokale System ein Schlüsselpaar, sofern dies noch nicht vorhanden ist.
- Durchführbare Aktionen mit persönlichem Zertifikat:
  - betrachten,
  - exportieren oder
  - importieren.

Persönliche Zertifikate
Zertifikatsverwaltung unter Win2000

- Praktische Demonstration:
  - *MMC mit Snap-In „Zertifikate“ öffnen*
  - *Betrachtung der Eigenschaften eines Zertifikats*
  - *Persönliches Zertifikat sichern (Export)*
  - *Persönliches Zertifikat restaurieren (Import)*

Persönliche Zertifikate
Zertifikatsverwaltung im IE 5.x

- Praktische Demonstration:
  - *Internet Explorer 5.x:*
    - *Gespeicherte Zertifikate*
    - *Zertifikatsprüfung*
    - *Sicherheitseinstellungen*
    - *Zertifikats-Exploits (Sicherheitslücken)*
  - *Zertifikatsuntersuchung anhand der URL*
    https://webmail.t-online.de/

Gliederung

- Prolog
- Funktionen der Dateiverschlüsselung
- EFS-Features
- Dateien und Verzeichnisse verschlüsseln
- Persönliche Zertifikate verwalten
- Verschlüsselte Dateien wiederherstellen
- Wiederherstellungszertifikate verwalten
- Wiederherstellungsagenten hinzufügen
- Dateien auf Dateiservern verschlüsseln

Der Data Recovery Agent
Fremde Dateien lesen

- Die Standard-Identität des Datenwieder-herstellungs-Agenten ist wie folgt festgelegt:
  - Win 2K Pro (auch innerhalb einer Domäne): lokales Konto des Administrator
  - Eigenständiger Win 2K Server: lokales Konto des Administrator
  - Win 2K DC oder Mitgliedsserver: AD-Konto Administrator

Gliederung

- Prolog
- Funktionen der Dateiverschlüsselung
- EFS-Features
- Dateien und Verzeichnisse verschlüsseln
- Persönliche Zertifikate verwalten
- Verschlüsselte Dateien wiederherstellen
- Wiederherstellungszertifikate verwalten
- Wiederherstellungsagenten hinzufügen
- Dateien auf Dateiservern verschlüsseln

Wiederherstellungszertifikate
Verwaltung

- Warum DRA-Zertifikate verwalten?
- Praxis:
  - *Sicherung des Zertifikats und Schlüssels eines DRA an einer Arbeitsstation*
  - *Wiederherstellung gesicherter Zertifikate und Schlüssel eines DRA an einer Arbeitsstation*

Gliederung

- Prolog
- Funktionen der Dateiverschlüsselung
- EFS-Features
- Dateien und Verzeichnisse verschlüsseln
- Persönliche Zertifikate verwalten
- Verschlüsselte Dateien wiederherstellen
- Wiederherstellungszertifikate verwalten
- Wiederherstellungsagenten hinzufügen
- Dateien auf Dateiservern verschlüsseln

DRA-Accounts verwalten
Weitere DRAs einrichten

- DRA-Konten werden in den Gruppenricht-linien festgelegt
- Diese Richtlinien werden über das Gruppen-richtlinien-Snap-In gpedit.msc definiert

Gliederung

- Prolog
- Funktionen der Dateiverschlüsselung
- EFS-Features
- Dateien und Verzeichnisse verschlüsseln
- Persönliche Zertifikate verwalten
- Verschlüsselte Dateien wiederherstellen
- Wiederherstellungszertifikate verwalten
- Wiederherstellungsagenten hinzufügen
- Dateien auf Dateiservern verschlüsseln

Verschlüsselung auf Server
Vorüberlegung

Durch den Mechanismus der einzelnen Dienste, die bei der Verschlüsselung mitwirken, können auf Dateiservern gespeicherte Dateien und Verzeichnisse nicht ohne weitreichende Vorbereitung chiffriert werden.

Es muss einen Server geben, dem die Schlüssel und Zertifikate der Benutzer bekannt sind, so dass diese über das Netzwerk verteilt werden können. Dies ist der Zertifikatsserver.

Verschlüsselung auf Server
Der Zertifikatsserver

- Praxis:
  - Installation des Zertifikatsservers
  - Konfiguration eines Zertifikatsservers

- **Weiterführende Verweise**
  - Grundlagen Kryptographie
  - Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste
  - Verordnung zur digitalen Signatur
  - DES
  - Kostenfreie CA-Nutzung für Privatanwender mit PGP
  - Quantenkryptographie