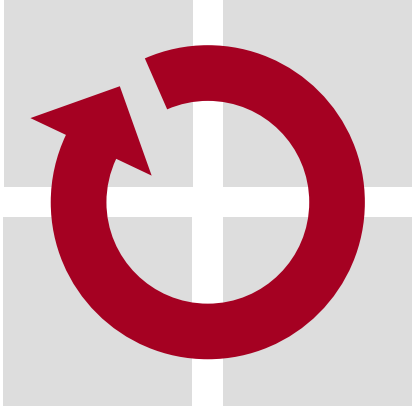
NTFS Encrypting File System

Markus Gerstner

Lehrstuhl für Informatik 4
Verteilte Systeme und Betriebssysteme
Universität Erlangen-Nürnberg



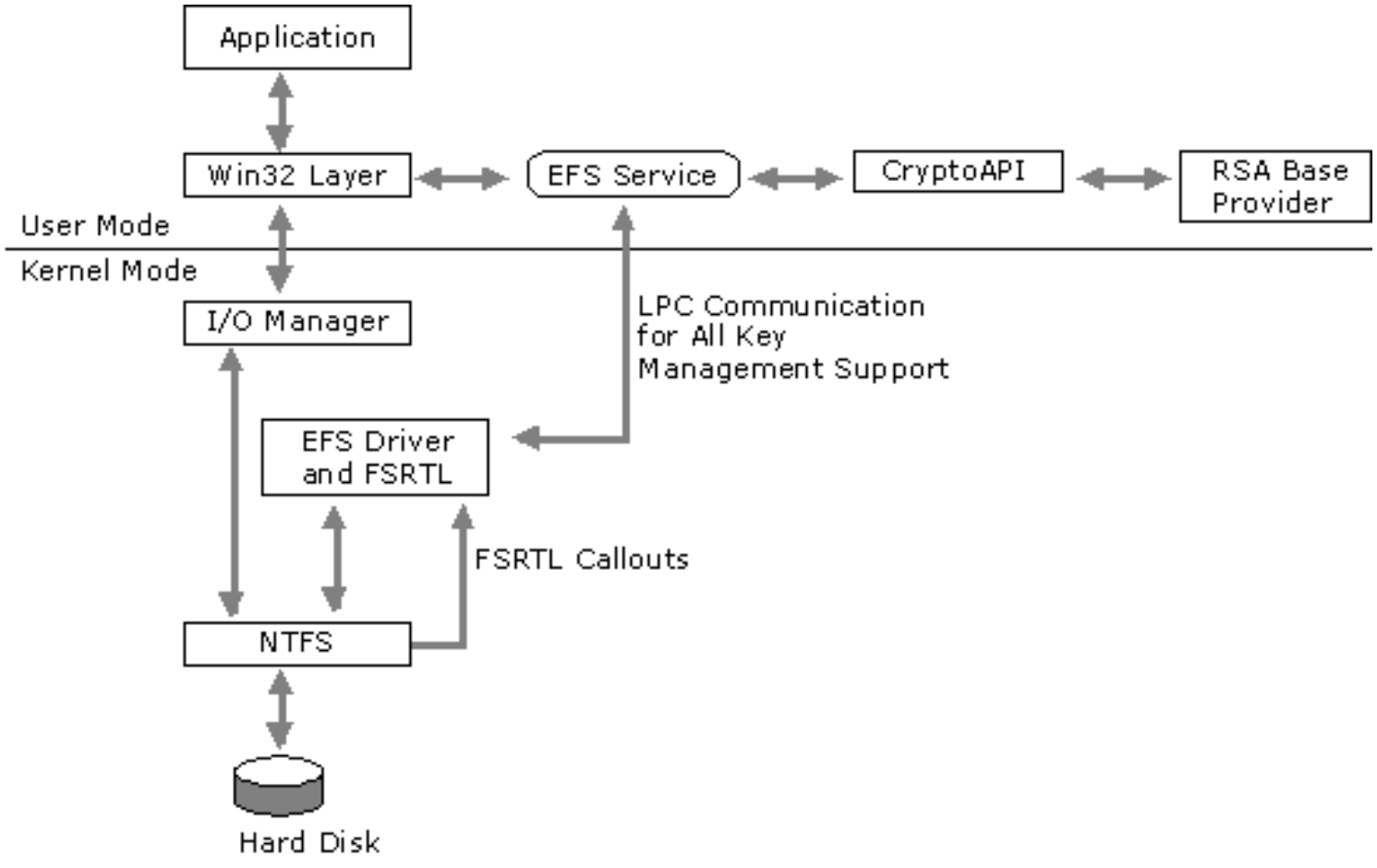
Überblick

- Was genau ist EFS?
- Warum EFS?
- Das Verschlüsselungsverfahren
- Benutzung
- Sicherheit
- Fazit

EFS: Begriff

- Erweiterung des NTFS-Dateisystems unter Microsoft Windows
- Ermöglicht verschlüsseltes Speichern
- Seit Windows 2000

EFS Architektur



Warum EFS?

- Motivation: Datei-Inhalte sollen nur für autorisierte Personen einsehbar sein

Warum EFS?

- Motivation: Datei-Inhalte sollen nur für autorisierte Personen einsehbar sein
- Problem: Angreifer mit physischem Zugang zum Rechner/Datenträger kann Zugriffskontrolle umgehen

Warum EFS?

- Motivation: Datei-Inhalte sollen nur für autorisierte Personen einsehbar sein
- Problem: Angreifer mit physischem Zugang zum Rechner/Datenträger kann Zugriffskontrolle umgehen
- Lösung: Dateien werden verschlüsselt gespeichert

Warum EFS?

- Motivation: Datei-Inhalte sollen nur für autorisierte Personen einsehbar sein
- Problem: Angreifer mit physischem Zugang zum Rechner/Datenträger kann Zugriffskontrolle umgehen
- Lösung: Dateien werden verschlüsselt gespeichert
- Frage: Warum Verschlüsselung nicht durch Anwendung, sondern durch das Betriebssystem?

Vorteile der BS-Lösung

- Transparenz: Ver- und Entschlüsselung geschieht automatisch beim Dateizugriff

Vorteile der BS-Lösung

- Transparenz: Ver- und Entschlüsselung geschieht automatisch beim Dateizugriff
- Automatische Verschlüsselung temporär erzeugter Dateien

Vorteile der BS-Lösung

- Transparenz: Ver- und Entschlüsselung geschieht automatisch beim Dateizugriff
- Automatische Verschlüsselung temporär erzeugter Dateien
- Schlüssel können im nicht auslagerbaren Speicher gehalten werden

Das Verschlüsselungsverfahren

- Kombination aus symmetrischem und asymmetrischem Algorithmus

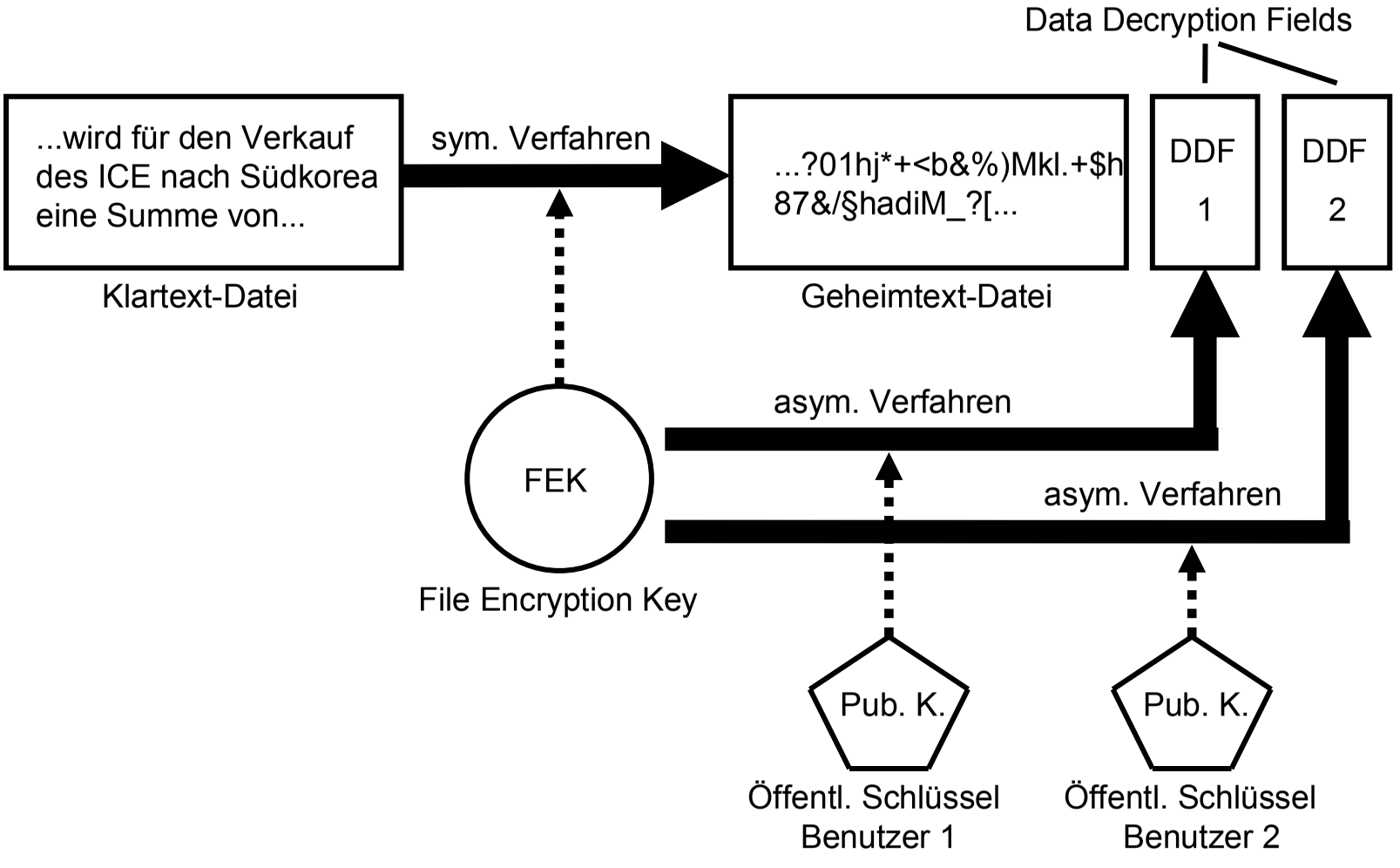
Das Verschlüsselungsverfahren

- Kombination aus symmetrischem und asymmetrischem Algorithmus
- Symmetrische Algorithmen:
  - Ver- und entschlüsselt wird mit dem gleichen Schlüssel
  - In der Regel sehr schnell

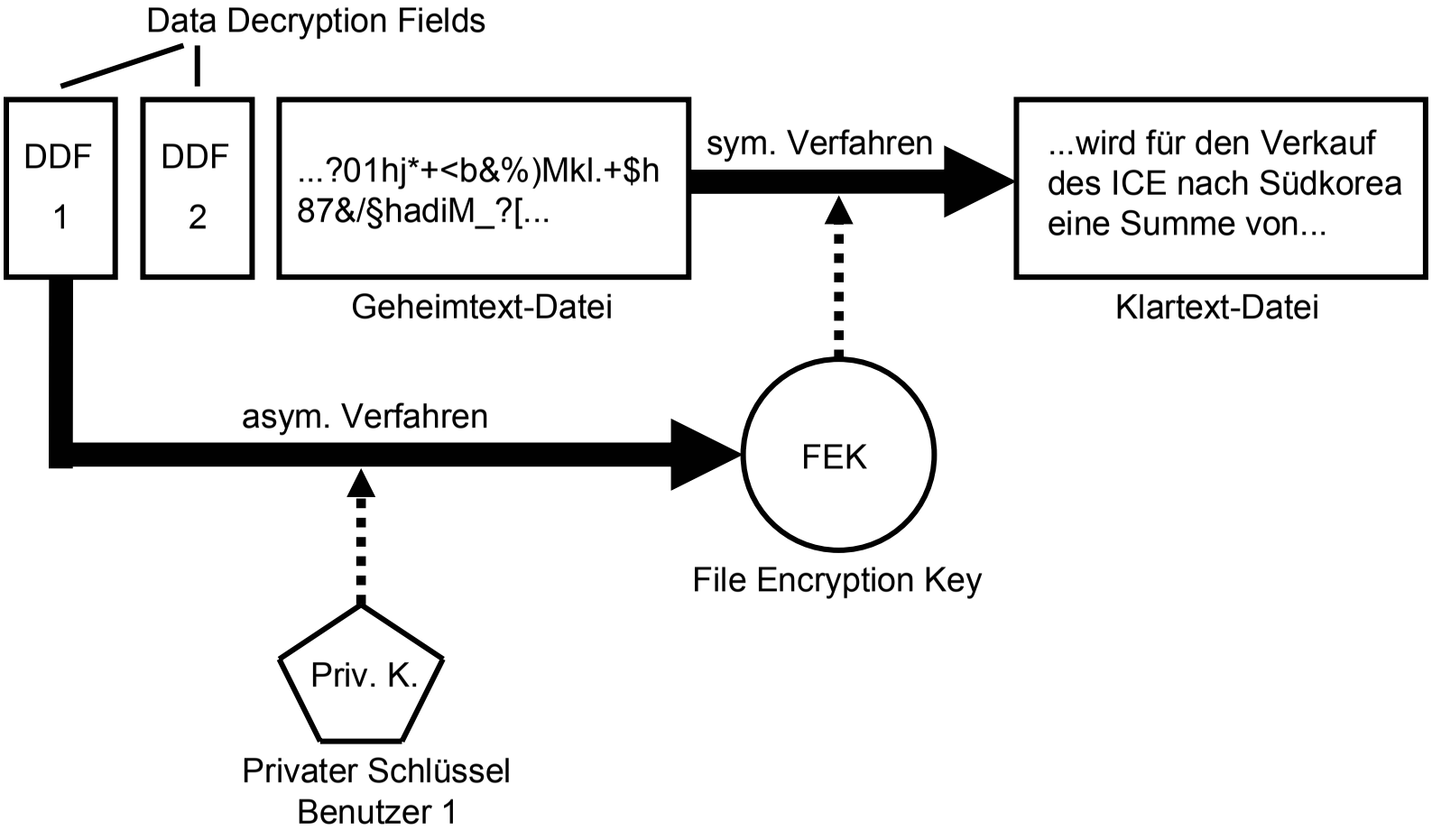
Das Verschlüsselungsverfahren

- Kombination aus symmetrischem und asymmetrischem Algorithmus
- Symmetrische Algorithmen:
  - Ver- und entschlüsselt wird mit dem gleichen Schlüssel
  - In der Regel sehr schnell
- Asymmetrische Algorithmen:
  - Verschlüsselung mit einem Schlüssel, Entschlüsselung mit einem anderen
  - In der Regel zeitaufwendig

Verschlüsselung von Dateien



Entschlüsselung von Dateien



Die Algorithmen

- Symmetrische Verfahren: Varianten von DES mit wesentlich längeren Schlüsseln
  - DESX: 120-Bit-Schlüssel
  - 3DES: 112-Bit-Schlüssel
  - Zum Vergleich: DES arbeitet mit 56-Bit-Schlüssel

Die Algorithmen

- Symmetrische Verfahren: Varianten von DES mit wesentlich längeren Schlüsseln
  - DESX: 120-Bit-Schlüssel
  - 3DES: 112-Bit-Schlüssel
  - Zum Vergleich: DES arbeitet mit 56-Bit-Schlüssel
- Asymmetrisches Verfahren: RSA
  - >= 512-Bit-Schlüssel

Benutzung von EFS (1)

- Dateien können das Attribut „verschlüsselt“ bekommen

Benutzung von EFS (1)

- Dateien können das Attribut „verschlüsselt“ bekommen
- Verzeichnisse können ebenfalls als „verschlüsselt“ gekennzeichnet werden
  - Neu im Verzeichnis erschaffene Dateien werden verschlüsselt
  - In das Verzeichnis kopierte Dateien werden verschlüsselt

Benutzung von EFS (1)

- Dateien können das Attribut „verschlüsselt“ bekommen
- Verzeichnisse können ebenfalls als „verschlüsselt“ gekennzeichnet werden
  - Neu im Verzeichnis erschaffene Dateien werden verschlüsselt
  - In das Verzeichnis kopierte Dateien werden verschlüsselt
- Empfehlung: Immer Verzeichnisse verschlüsseln

Benutzung von EFS (2)

- Verschieben in verschlüsseltes Verzeichnis bedeutet nicht automatisch Verschlüsselung

Benutzung von EFS (2)

- Verschieben in verschlüsseltes Verzeichnis bedeutet nicht automatisch Verschlüsselung
- Speichern auf Nicht-NTFS-Partitionen bedeutet Verlust der Verschlüsselung

Benutzung von EFS (2)

- Verschieben in verschlüsseltes Verzeichnis bedeutet nicht automatisch Verschlüsselung
- Speichern auf Nicht-NTFS-Partitionen bedeutet Verlust der Verschlüsselung
- Keine verschlüsselte Übertragung über das Netzwerk

Benutzung von EFS (2)

- Verschieben in verschlüsseltes Verzeichnis bedeutet nicht automatisch Verschlüsselung
- Speichern auf Nicht-NTFS-Partitionen bedeutet Verlust der Verschlüsselung
- Keine verschlüsselte Übertragung über das Netzwerk
- Systemdateien können nicht verschlüsselt werden

Zertifikate & Schlüssel

- Benutzer benötigt EFS-Zertifikat und privaten Schlüssel
  - Zertifikat enthält öffentlichen Schlüssel
  - Zertifikat ist einsehbar

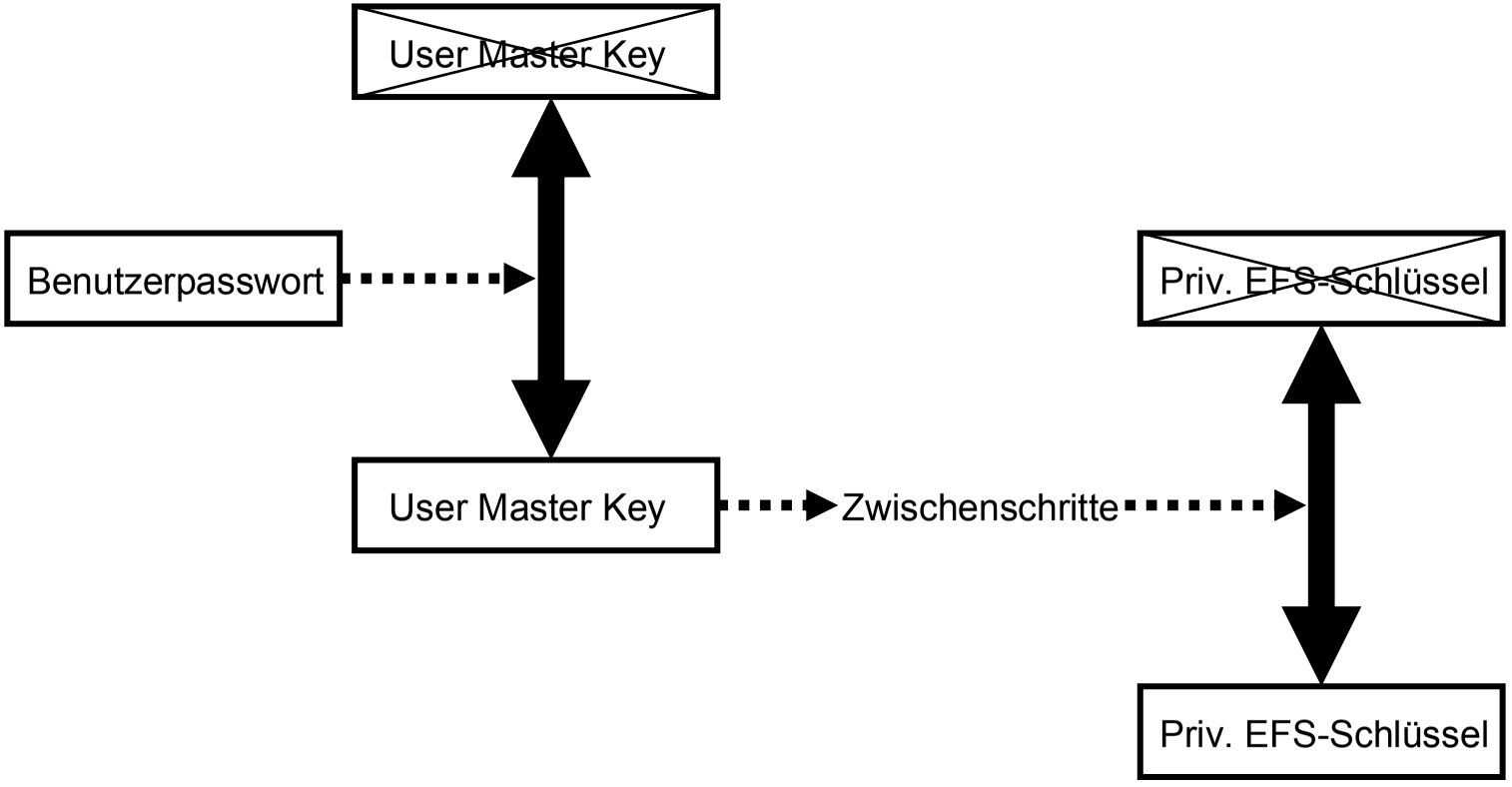
Zertifikate & Schlüssel

- Benutzer benötigt EFS-Zertifikat und privaten Schlüssel
  - Zertifikat enthält öffentlichen Schlüssel
  - Zertifikat ist einsehbar
- Beides wird in seinem Account gespeichert
  - Auffindbar unter \Documents and Settings\<username>\...
  - Kann auf dem Domaincontroller gespeichert sein und wird beim Login von dort heruntergeladen

Zertifikate & Schlüssel

- Benutzer benötigt EFS-Zertifikat und privaten Schlüssel
  - Zertifikat enthält öffentlichen Schlüssel
  - Zertifikat ist einsehbar
- Beides wird in seinem Account gespeichert
  - Auffindbar unter \Documents and Settings\<username>\...
  - Kann auf dem Domaincontroller gespeichert sein und wird beim Login von dort heruntergeladen
- Privater Schlüssel muss geschützt werden
  - Verschlüsselung indirekt über Benutzerpasswort

Schutz des privaten Schlüssels



Export von Schlüsseln

- Wichtig: Export von EFS-Zertifikaten und privaten Schlüsseln auf externe Datenträger möglich

Mehrbenutzerzugriff

- Benutzer mit Schreibrechten kann Datei verschlüsseln
- Benutzer kann dann weitere Benutzer auswählen, die Einsicht in die Datei haben sollen

Recovery Agents

- Verschlüsselung birgt immer Risiko des Datenverlustes

Recovery Agents

- Verschlüsselung birgt immer Risiko des Datenverlustes
- Z.B.: Benutzer verliert Schlüssel oder chiffriert böswillig Dateien

Recovery Agents

- Verschlüsselung birgt immer Risiko des Datenverlustes
- Z.B.: Benutzer verliert Schlüssel oder chiffriert böswillig Dateien
- Lösung: Recovery Agents
  - Ausgewiesene Benutzer, die alle Dateien in einem bestimmten Bereich entschlüsseln können
  - Jede verschlüsselte Datei bekommt zweiten Key Ring mit Einträgen für die Recovery Agents

Recovery Agents

- Verschlüsselung birgt immer Risiko des Datenverlustes
- Z.B.: Benutzer verliert Schlüssel oder chiffriert böswillig Dateien
- Lösung: Recovery Agents
  - Ausgewiesene Benutzer, die alle Dateien in einem bestimmten Bereich entschlüsseln können
  - Jede verschlüsselte Datei bekommt zweiten Key Ring mit Einträgen für die Recovery Agents
- Windows 2000 forciert Vorhandensein von Recovery Agents (XP nicht mehr)

Ablauf von Zertifikaten & Schlüsseln

- Zertifikate und Schlüssel werden unter bestimmten Umständen durch neue ersetzt (z.B.: „Verfallsdatum“)
  - Information in einer Datei wird beim ersten Zugriff nach dem Wechsel angepasst
  - Voraussetzung: Alte Zertifikate und Schlüssel noch vorhanden

Ablauf von Zertifikaten & Schlüsseln

- Zertifikate und Schlüssel werden unter bestimmten Umständen durch neue ersetzt (z.B.: „Verfallsdatum“)
  - Information in einer Datei wird beim ersten Zugriff nach dem Wechsel angepasst
  - Voraussetzung: Alte Zertifikate und Schlüssel noch vorhanden
- Daher: Archivieren der Zertifikate und Schlüssel, wenigstens für die Recovery Agents

Sicherheit von EFS

- DES und RSA gelten als sicher
- Lange DESX und 3DES-Schlüssel vereiteln Brute-Force-Angriffe
  - 120 bzw. 112-Bit-Schlüssel statt 56 Bit beim klassischen DES
  - Internationale EFS-Version vormals nur mit 40-Bit-Schlüssel!
- Lücken ergeben sich eher an anderen Stellen

Klartextreste

- Temporäre Dateien
  - EFS erzeugt beim erstmaligen Verschlüsseln einer Datei eine Kopie, die nicht überschrieben wird
  - Anwendungen erzeugen temporäre Dateien in Temp- oder Spool-Verzeichnissen → Diese Verzeichnisse verschlüsseln!

Klartextreste

- Temporäre Dateien
  - EFS erzeugt beim erstmaligen Verschlüsseln einer Datei eine Kopie, die nicht überschrieben wird
  - Anwendungen erzeugen temporäre Dateien in Temp- oder Spool-Verzeichnissen → Diese Verzeichnisse verschlüsseln!
- Auslagerungsdatei
  - Enthält Klartext
  - System kann so eingestellt werden, dass Auslagerungsdatei beim Herunterfahren überschrieben wird.

Sicherheitsfaktor Benutzerpasswort

- EFS gerade so stark, wie die Benutzerpasswörter
  - Unbedingt starke Passwörter durchsetzen
  - Sicherste Lösung: Zertifikate und Schlüssel exportieren und vom Rechner löschen
  - Export auf Smartcards möglich

Sicherheitsfaktor Benutzerpasswort

- EFS gerade so stark, wie die Benutzerpasswörter
  - Unbedingt starke Passwörter durchsetzen
  - Sicherste Lösung: Zertifikate und Schlüssel exportieren und vom Rechner löschen
  - Export auf Smartcards möglich
- Unter Windows 2000 Zugriff durch Rücksetzen der Passwörter möglich
  - Eklatantes Sicherheitsloch
  - Maßnahme dagegen: Verwendung von Syskey
    - Systempasswort wird vor dem Login verlangt
    - Kodierung der Passwortdatenbank
  - Sicherste Lösung: Zertifikate und Schlüssel exportieren

Zugriff durch Recovery Agents

- Recovery Agents haben Zugriff auf große Zahl von Dateien
  - Missbrauch besonders schwerwiegend
  - Verhindern des Zugriffs durch Export der Zertifikate und Schlüssel

Fazit

- Zurückbleiben von Klartext auf dem Datenträger ein Mangel
- Dennoch: Angreifer hat zumindest höheren Aufwand, um an Daten zu kommen
- Einfache Benutzung

Wichtigste Quellen (1)

- Schneier, B.,
  Applied Cryptography,
  Protocols, Algorithms, and Source Code in C,
  Second Edition, John Wiley & Sons, Inc 1996

- Wobst, R.,
  Abenteuer Kryptologie,
  Methoden, Risiken und Nutzen der Datenverschlüsselung,
  2., überarbeitete Auflage, Addison Wesley Longman Verlag GmbH 1998

- Russinovich, M.,
  Inside Encrypting File System, Part 1
  http://www.winntmag.com/Articles/Index.cfm?ArticleID=5387&pg=1&show=1214
  Windows & .NET Magazine 1999

Wichtigste Quellen (2)

- Microsoft Windows 2000 Professional,
  Die technische Referenz,
  Microsoft Press Deutschland 2000

- Microsoft Windows 2000 Server Resource Kit,
  Distributed Systems Guide – Chapter 15 – Encrypting File System,
  http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/reskit/distsys/part2/dsgch15.asp,
  Microsoft Corporation 2003

- Encrypting File System in Windows XP and Windows Server,
  http://www.microsoft.com/windowsxp/pro/techinfo/administration/recovery/EncryptingFileSystem.doc,
  Microsoft Corporation 2002