

ISSS Zürcher Tagung 2009

# **DRM in der Unternehmung: Beispiel Microsoft RMS**

IWI Institut für Wirtschaftsinformatik

**Armand Portmann**

dipl. El. Ing. ETH

[armand.portmann@hslu.ch](mailto:armand.portmann@hslu.ch)

17. Juni 2009

# Agenda

- Einleitung
- Funktion
- Anwendung
- Chancen und Risiken
- Demo

# Agenda

- Einleitung
- Funktion
- Anwendung
- Chancen und Risiken
- Demo

## Begriff: Enterprise Rights Management

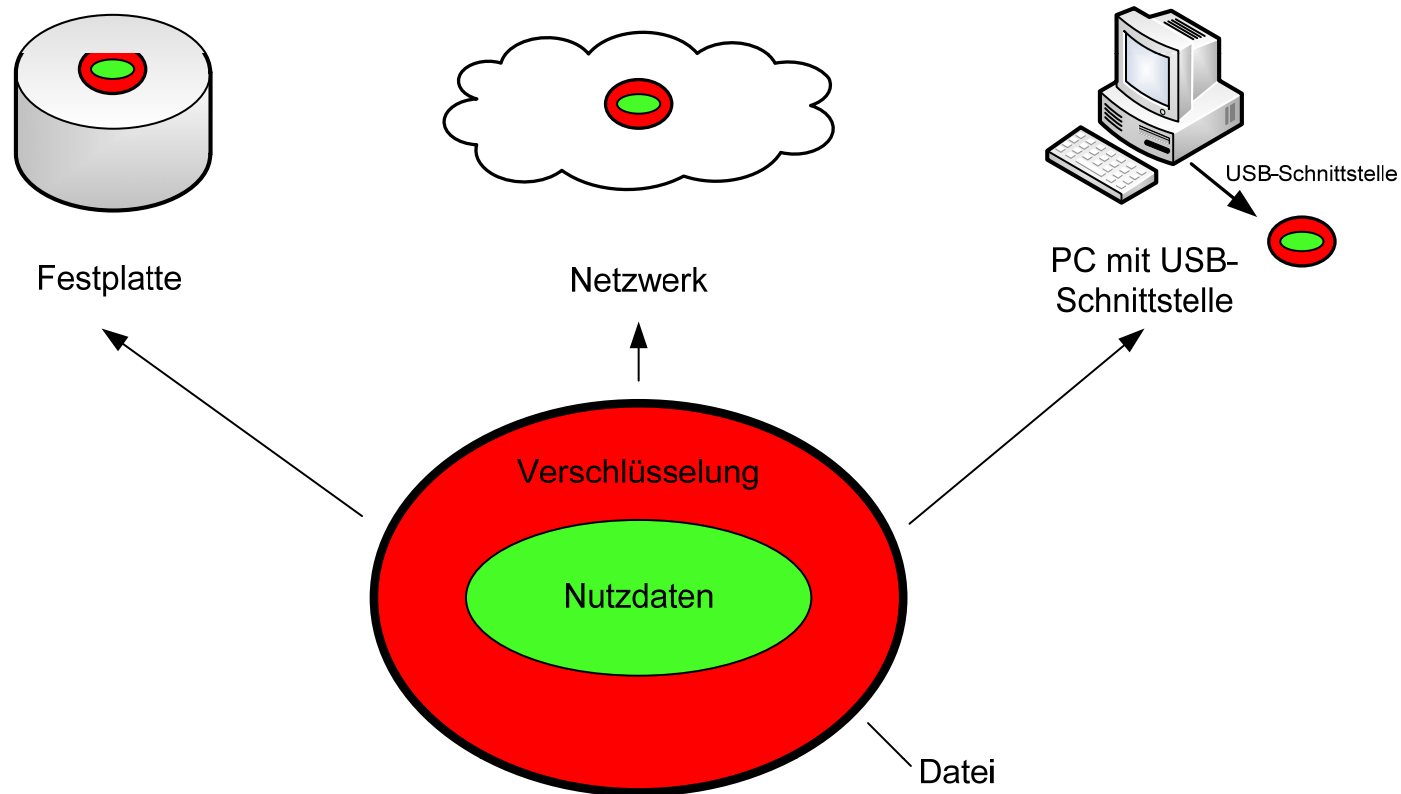
- Technologie zum Schutz sensibler Firmendaten, z. B. Office Dokumente (Word, PowerPoint, etc.)
- Produkte
  - Adobe LiveCycle Rights Management
  - EMC Documentum Information Rights Management (vormals Authentica Active Rights Management)
  - Oracle Information Rights Management
  - *Microsoft Rights Management Services*

## Motivation

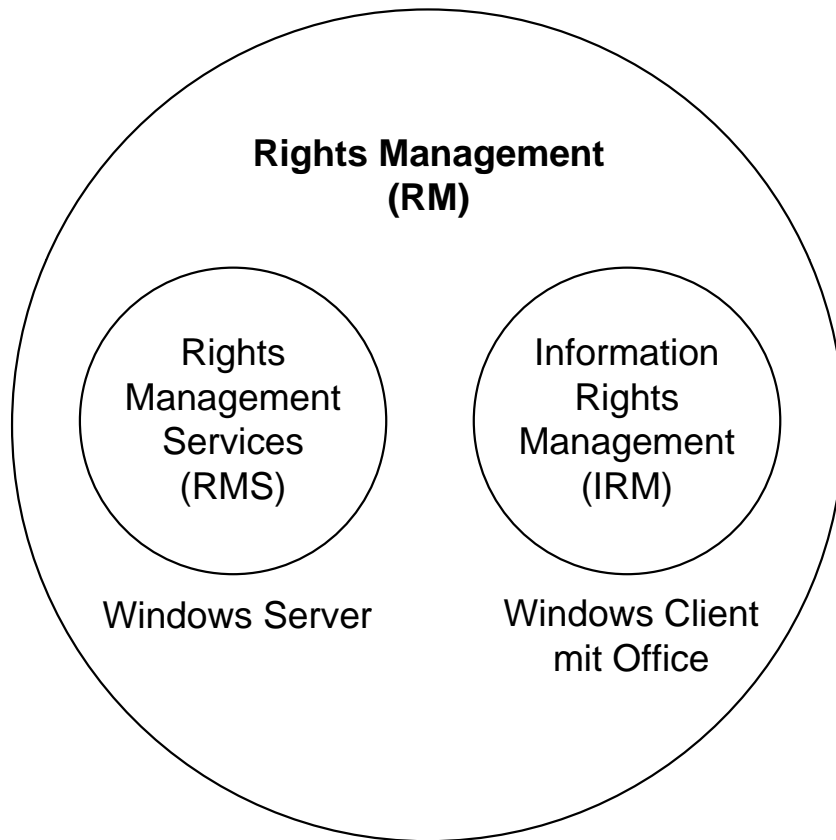
- Traditionellerweise werden Daten an ihrem Ablageort oder auf dem Transportweg geschützt
- Das Wegkopieren sensibler Daten wird durch eine Kontrolle der USB-Ports zu verhindern versucht
- Die Umsetzung eines lückenlosen Schutzes ist sehr schwierig
- Schlupflöcher bleiben immer: Ein berechtigter Benutzer kann z. B. eine verschlüsselte Datei unverschlüsselt abspeichern und weitergeben
- Enterprise Rights Management Systeme bieten eine elegante Lösung für diese Probleme

# Lösung

- Den Schutz einer Datei – d. h. die Verschlüsselung – *untrennbar* mit der Datei verbinden



# Microsoft RMS - Terminologie



- Rights Management Services (RMS) beschreibt nur einen Teil eines grösseren Systems
- Trotzdem wird in der Regel von RMS gesprochen, wenn das Gesamtsystem gemeint ist

## Microsoft RMS - Terminologie

- Rights Management Services (RMS)
  - Server-Komponente, die unter Windows Server 2003 oder 2008 läuft
  - Unter Server 2008 heisst die Komponente neu *Active Directory Rights Management Services* (AD RMS)
- Information Rights Management (IRM)
  - Client-Komponente, die unter Windows XP oder Vista läuft und Office 2003 oder Office 2007 Dokumente schützt

## Microsoft RMS - Facts

- Systemvoraussetzungen
  - Server-Seite: Windows Server, Active Directory, SQL-Datenbank
  - Client-Seite: Windows XP oder Vista + RMS-fähige Appl.
- RMS-fähige Applikationen von Microsoft
  - Word, Excel, PowerPoint, Outlook (E-Mail!)
  - SharePoint Server (ab RMS 2003 SP 2)
- Es lassen sich *nicht* beliebige Dateien schützen
- Mithilfe eines SDK lassen sich eigene RMS-fähige Applikationen entwickeln

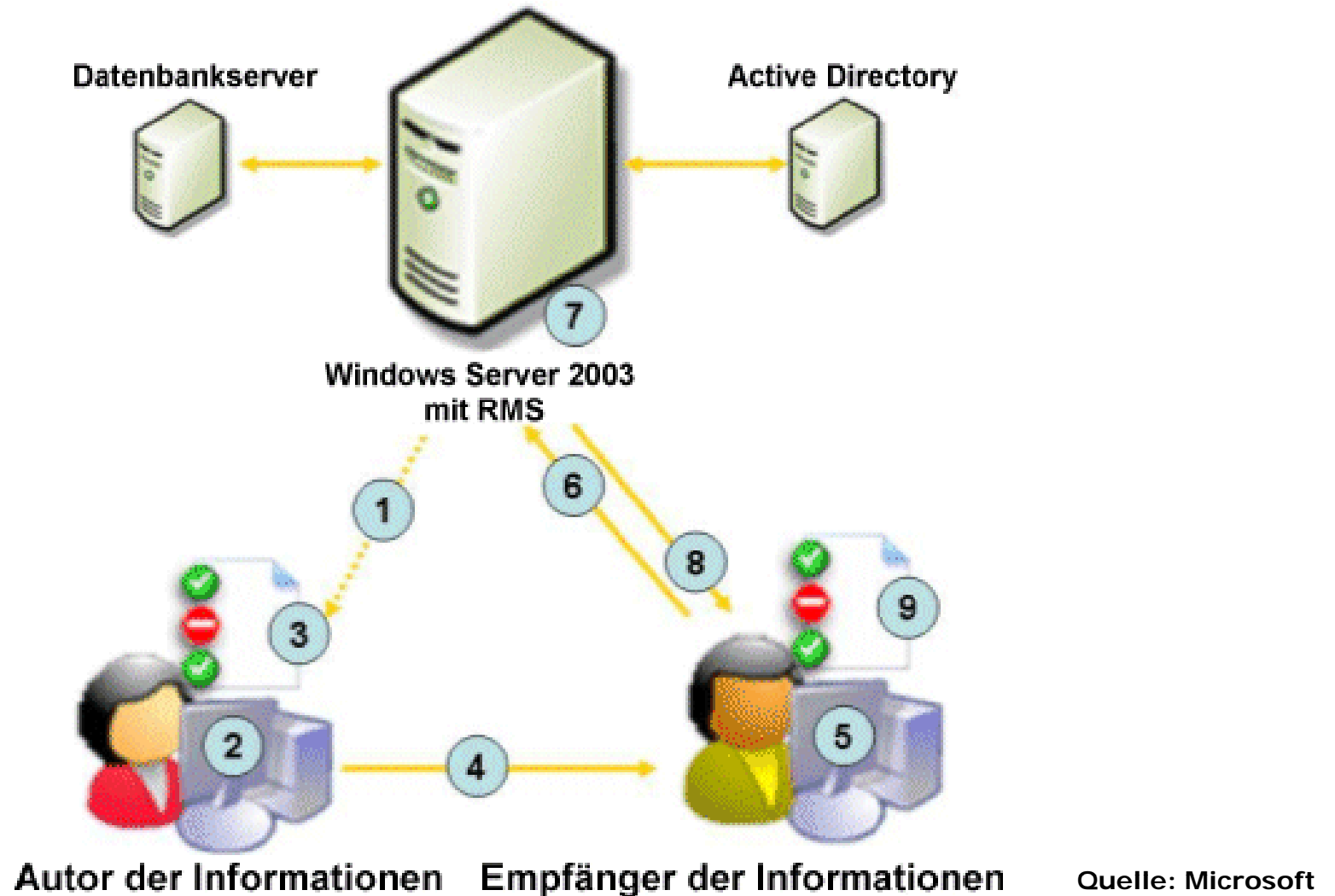
## Microsoft RMS - Facts

- Dritthersteller bieten RMS-fähige Applikationen an
  - Für PDF-Files: GigaTrust Corp. ([www.gigatruster.com](http://www.gigatruster.com))
- RMS ist FIPS 140-2 Level 1 zertifiziert (ab RMS 2003 SP 1)
- Schlüsselmaterial des RMS-Servers lässt sich auf HSMs ablegen (HW-based CSP, z. B. nCipher netHSM)
- AD RMS lässt sich firmenübergreifend nutzen
- Es ist möglich, auch auf nicht AD-Clients RMS zu verwenden

# Agenda

- Einleitung
- **Funktion**
- Anwendung
- Chancen und Risiken
- Demo

# Abläufe bei der Verwendung von RMS



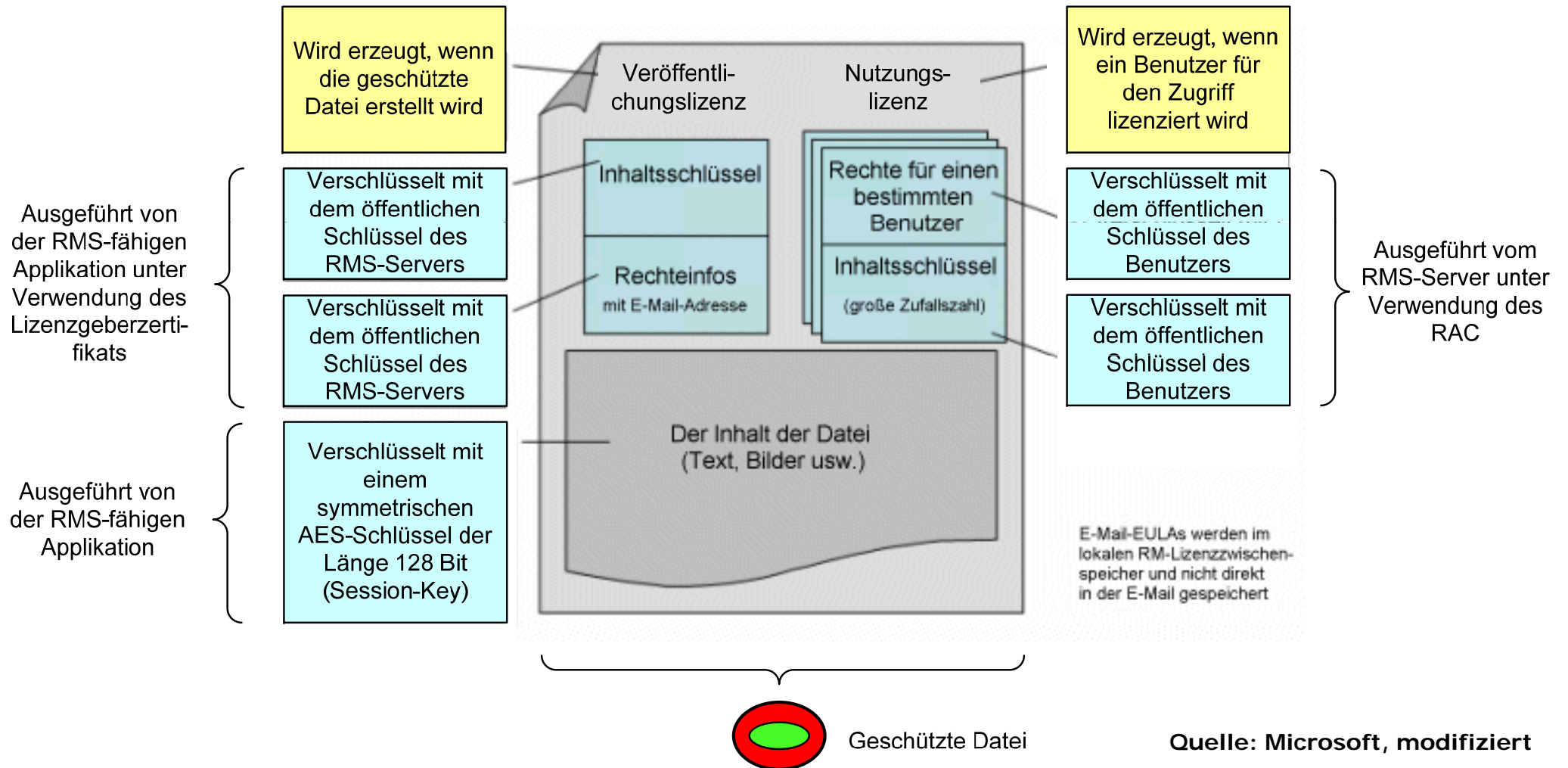
## Abläufe bei der Verwendung von RMS

1. Einmalige Registrierung des Client-Computers beim RMS-Server
2. Erstellung einer zu schützenden Datei mithilfe einer RMS-fähigen Applikation und Definition der Nutzungsbedingungen
3. Hinzufügen einer Veröffentlichungslizenz zur Datei (Lizenz enthält die Nutzungsbedingungen)
4. Verteilung der Datei über einen beliebigen Kanal
5. Öffnen der Datei mithilfe einer RMS-fähigen Applikation (und gegebenenfalls einmalige Registrierung des Client-Computers)

## Abläufe bei der Verwendung von RMS

6. Beantragen einer Nutzungslizenz beim RMS-Server
7. Prüfung der Autorisierung des Empfängers durch den RMS-Server und Erstellung der entsprechenden Nutzungslizenz
8. Übertragung der Nutzungslizenz auf den Client-Computer
9. Prüfung der Nutzungslizenz und Öffnen der Datei mit den entsprechenden Berechtigungen

# Aufbau einer geschützten Datei



Quelle: Microsoft, modifiziert

# Agenda

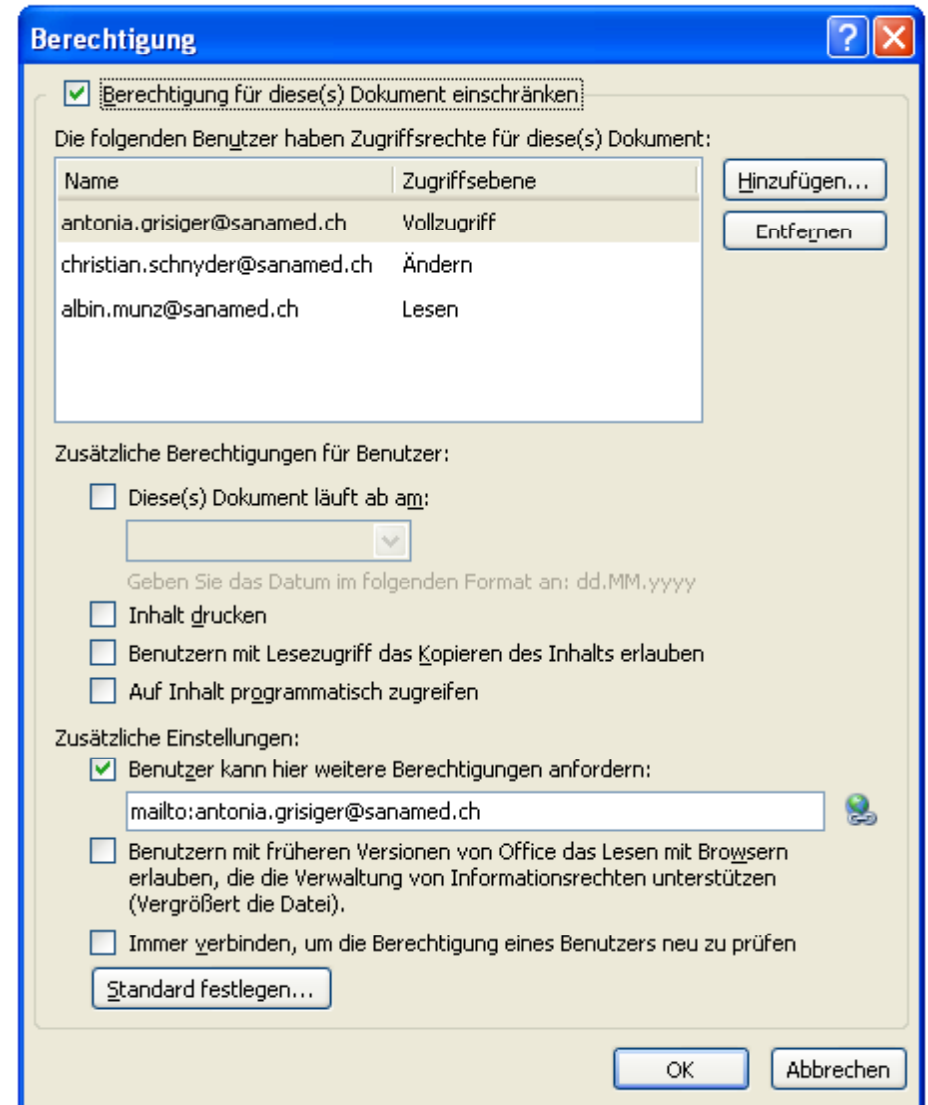
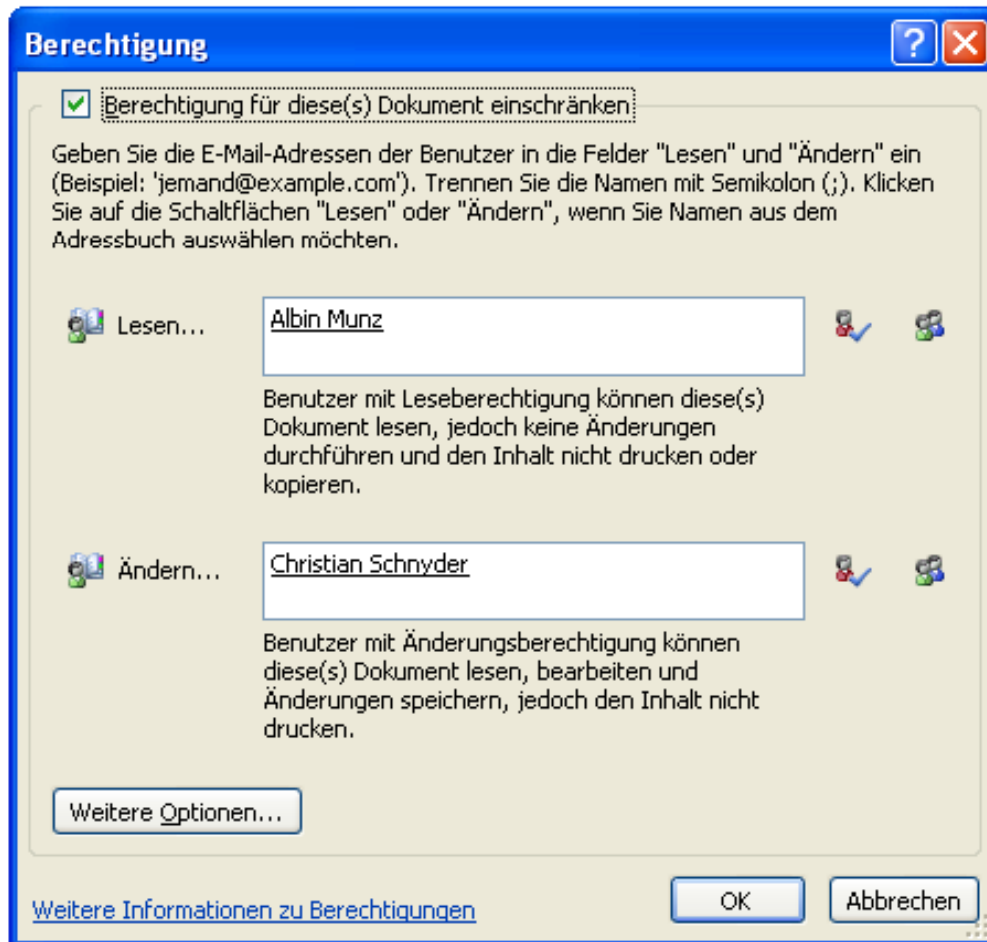
- Einleitung
- Funktion
- **Anwendung**
- Chancen und Risiken
- Demo

# In Office konfigurierbare Datei-Berechtigungen

- Lesen
  - Bearbeiten
  - Speichern/speichern unter
  - Inhalte in Zwischenablage kopieren
  - Makros ausführen
  - Berechtigungen lesen
  - Drucken
  - Setzen eines Ablaufdatums
- 
- Hinweis: Benutzer werden über deren E-Mail Adresse selektiert

# In Office konfigurierbare Datei-Berechtigungen

Menüpunkt: *Datei / Berechtigung* in Word

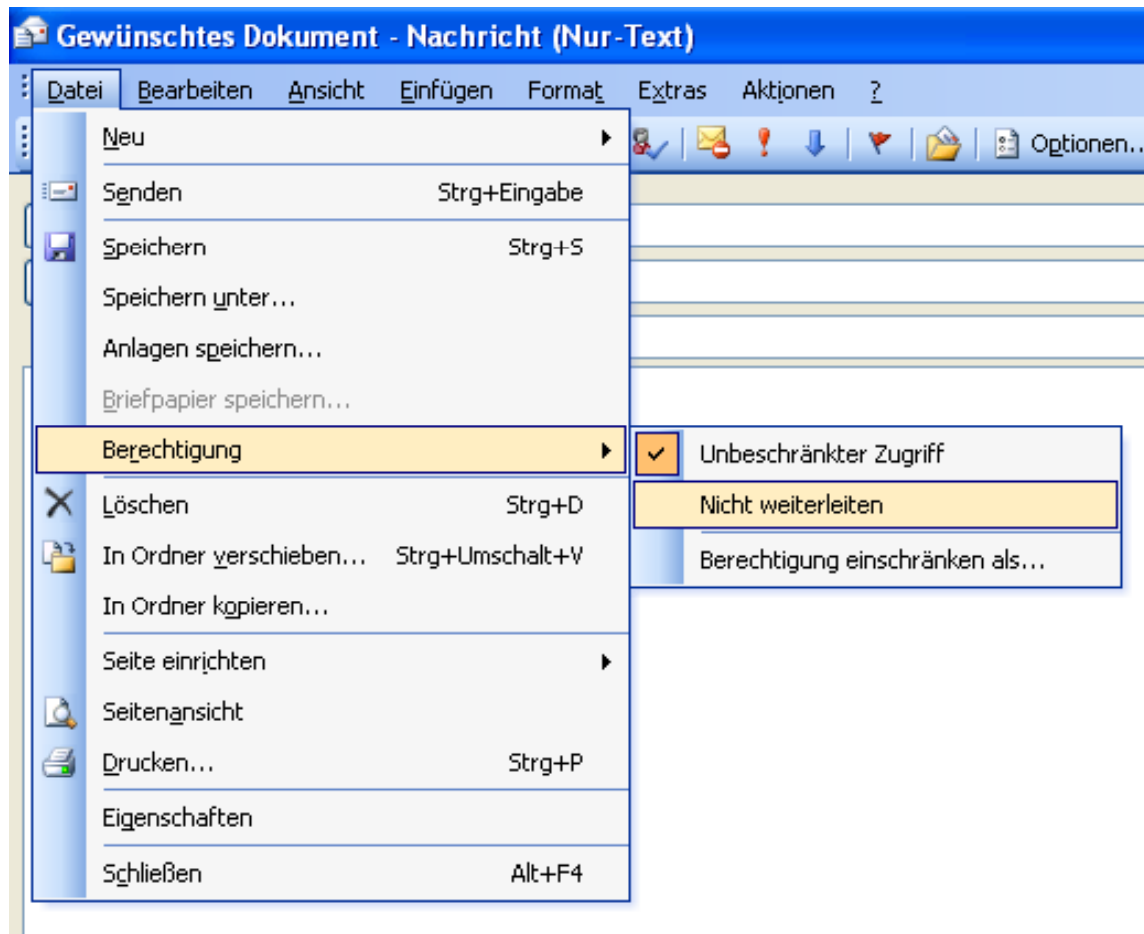


# In Outlook konfigurierbare E-Mail Berechtigungen

- Antworten erlaubt/nicht erlaubt
- Allen Antworten erlaubt/nicht erlaubt
- Weiterleiten erlaubt/nicht erlaubt
  
- Hinweise
  - RMS-geschützte E-Mails sind immer verschlüsselt
  - Dateianhänge erben den RMS-Schutz von der E-Mail (Empfänger bekommt eine Lese-Berechtigung auf dem Dokument)
  - Im Standard-Dialog lässt sich nur die Berechtigung Weiterleiten erlaubt/nicht erlaubt konfigurieren

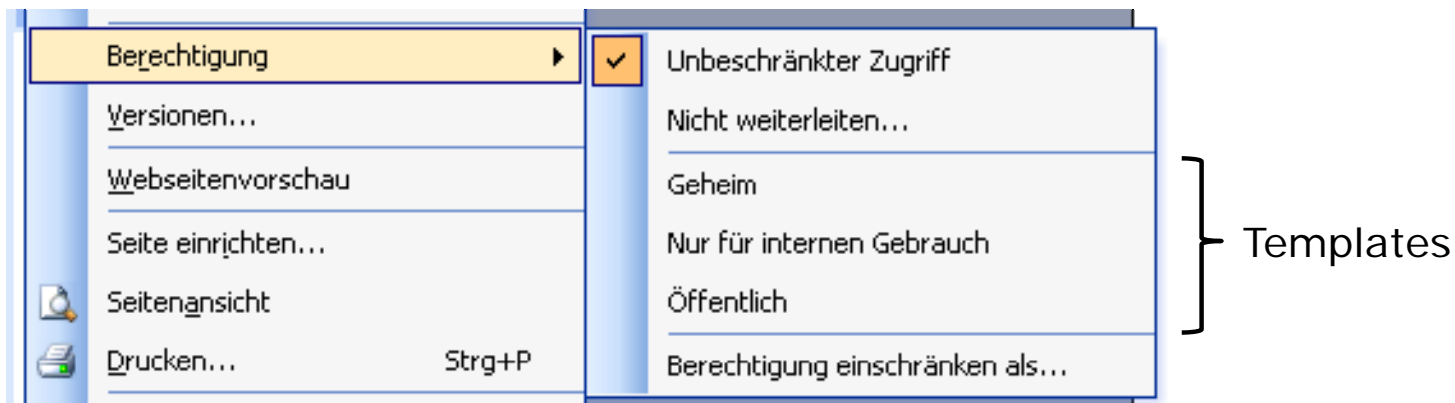
# In Outlook konfigurierbare E-Mail Berechtigungen

Menüpunkt: *Datei / Berechtigung* in Outlook



# Templates

- Templates bestehen aus einer vordefinierten Menge von Berechtigungen
- Sie können Dateien oder E-Mails zugeordnet werden
- Dadurch können komplexe Berechtigungs-Sets einfach auf Dateien oder E-Mails angewendet werden
- Mithilfe von Templates kann z. B. ein Klassifikationsschema umgesetzt werden



# Agenda

- Einleitung
- Funktion
- Anwendung
- Chancen und Risiken
- Demo

## Chancen

- Umfassender Schutz (für Ablage, Transport, etc.), der untrennbar mit der Datei verbunden ist
- Hoher Sicherheitslevel (128 Bits symmetrisch, 1024 Bits asymmetrisch)
- Beinahe transparente Anwendung, von welcher der End-User nur wenig merkt
- Ziemlich einfacher Betrieb der RMS-Infrastruktur (es muss keine PKI aufgebaut und betrieben werden)
- Sinnvoller Einsatz setzt eine Datenklassifikation voraus

## Risiken

- Fehlkonfiguration: Bei fehlerhafter Vergabe von Berechtigungen können berechtigte Benutzer Dateien nicht entschlüsseln (d. h. lesen oder bearbeiten)
- Ungenügende Verfügbarkeit der RMS-Server: Ohne RMS-Server können geschützte Dateien nicht oder nur über einen beschränkten Zeitraum entschlüsselt werden
- Verlust des Schlüsselmaterials des RMS-Servers: Es können keine Nutzungslizenzen mehr ausgestellt werden (Dateien u. U. verloren)

## Risiken

- **Unsorgfältige Revokation:** Sie kann dazu führen, dass auch berechnigte Personen ihre Nutzungsrechte an Dateien verlieren
- **RMS-Admins:** Sie haben Vollzugriff auf sämtliche geschützten Dateien (aber auch sinnvoll, z. B. bei Austritt von Mitarbeitern)
- **Domain-Admins:** Sie können sich über ein Benutzerkonto Zugriff auf geschützte Dateien verschaffen (Passwort zurücksetzen genügt)

## Risiken

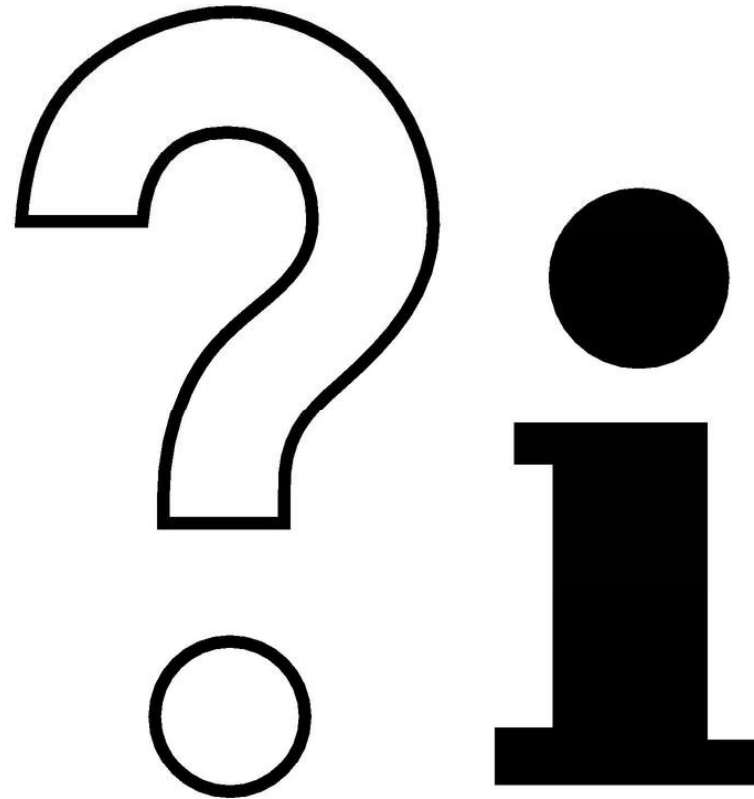
- Screen-Shots: Lassen sich nicht zu 100% verhindern (fotografieren geht sowieso immer)
- Auslagerungsdatei: Sie enthält u. U. entschlüsselte Inhalte (gemäss Microsoft TechNet-Dokumentation)
- Verbreitung der Technologie: Enterprise Rights Management Systeme sind noch nicht weit verbreitet; es sind deshalb eher wenig Erfahrungen in der Anwendung vorhanden

# Agenda

- Einleitung
- Funktion
- Anwendung (Windows XP, Office 2007)
- Chancen und Risiken
- Demo

# Demo

- Dateien schützen
- E-Mails schützen



[armand.portmann@hslu.ch](mailto:armand.portmann@hslu.ch)