

Was ist DRM?

CC Informations- & Softwaresicherheit

Roland Portmann

Leiter CC ISS

T direkt +41 41 349 33 83

roland.portmann@hslu.ch

Horw 22. Juni 2009

Begründung, Ziele, Anforderungen

DRM Digital Rights Management

- Schutz von Informationen mittels kryptologischen Verfahren
- Gründe für DRM
 - Klassische Zugriffsschutzmechanismen können nicht eingesetzt werden
 - Die Verwendung der Informationen soll eingeschränkt werden
- Klassisches DRM schützt:
 - Multimedia-Dateien
 - eBooks
 - Software
- Entstehung Mitte 90er Jahre

Klassische DRM-Systeme

- Verschiedene Anbieter:
 - Adobe Protected Streaming
 - FairPlay (Adobe iTunes)
 - Real Networks Helix (Open Source)
 - Microsoft Windows Media Digital Rights Management
 - Microsoft PlayReady (Codex unabhängig)
 - Nintendo Wii
- Breite Kritik und Unbehagen
 - Digital Right != Schweizerischem Recht
 - Viele Nachteile für Kunden
 - Inkompatibilitäten
 - Verlust gekaufter Werke (z.B keine Lizenzübertragung)
 - Fehlerhafte Software
 - Ungenügende Backup-Möglichkeiten
 - Datenschutzprobleme
- Viele Schwachstellen (Entfernen des DRM-Schutzes)
- Anwendung stark rückläufig
 - Vermehrte Verwendung von digitalen Wasserzeichen

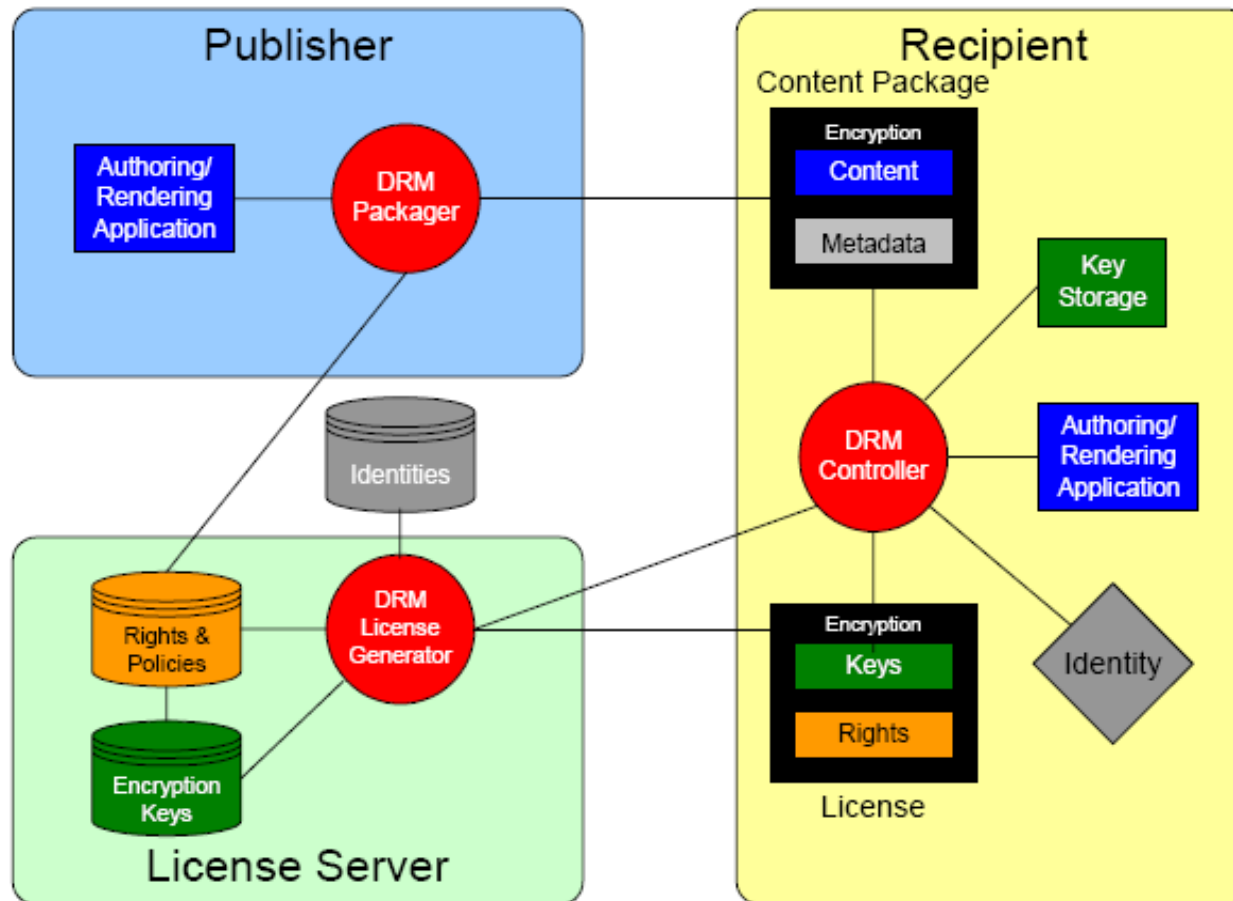
Enterprise Rights Management Basics

- Adaption der Technologie von DRM auf Unternehmensbedürfnisse
- Entstehung Ende 90er Jahre
- Allgemeine Ziele:
 - Schutz von betrieblichen Informationen
 - Ergänzung von bestehenden Zugriffsschutzmechanismen
 - Feingranulare Steuerung des Zugriffs auf Informationen
 - Einschränkungen bezüglich der Weiterverarbeitung von Informationen
 - Verhindern, dass Mitarbeiter den Zugriffsschutz umgehen können

Enterprise DRM – Warum?

- Klassische Zugriffsschutzsysteme haben definierte Grenzen
 - Systemgrenzen bei komplexen Organisationen immer schwieriger zu definieren
- Informationen können dupliziert werden.
 - Duplikate von Informationen sind ausserhalb der kontrollierten IT-Systeme
 - Beispiele: Notebook, USB-Stick, eMail, Portale, Handy
- Klassische Zugriffsschutzsysteme funktionieren nicht
 - Konzeptionelle Probleme
 - Betriebliche Probleme (Prozesse)
 - Reorganisation von Firmen
 - Schwachstellen von Betriebssystemen und Applikationen

ERM Referenz Architektur



Anforderung 1: Persistenter Schutz

- Schutz kann nicht entfernt oder umgangen werden
 - Kann nie vollständig erreicht werden.
 - Bildschirm kann fotografiert werden
 - Texterkennung von Screenshots
- Bestehende Systeme hatten teilweise Schwachstellen (beispielsweise Adobe DRM)
- Die gängigen Produkte erfüllen diese Anforderung

Anforderung 2: Schutz über Organisationsgrenzen hinweg

- Die Zugriffsregelung muss auch für organisationsfremde Personen definierbar sein
- Unterschiedliche Implementation bei verschiedenen Produkten:
 - Bei Microsoft RMS muss ein Trustverhältnis zwischen den Firmen aufgebaut werden. Benutzer basieren primär auf AD Benutzer
 - Andere Produkte haben eigene Benutzerverwaltungen
 - Meistens aber Zugriff auf den Licence Server notwendig
 - Local Caching der Credentials

Anforderung 3: Portabilität

- Zeitliche Portabilität
 - Zugriff auf Informationen zu beliebigen Zeiten
 - Hinweis: Zugriff zu bestimmten Zeiten kann auf unerlaubte Handlung hindeuten
- Rechner Portabilität
 - Zugriff ist nicht an bestimmten Rechner gebunden
 - Nicht in allen Fällen erwünscht
- Plattform Portabilität
 - Zugriff muss von verschiedenen Plattformen möglich sein
- Format Portabilität
 - Das Format muss verschiedenen Anwendungen angepasst werden können
 - Zugriff mit verschiedenen Applikationen auf die Informationen

Anforderung 4: Weiterverarbeitung der Informationen

- Informationen werden sehr häufig weiterverarbeitet.
 - Copy/Paste in andere Applikationen
 - Dokumente von verschiedenen Autoren müssen zusammengeführt werden können
- Die Weiterverarbeitung muss gesteuert werden können

Anforderung 5: Integration in Applikationen

- Ein ERM System sollte in die gebräuchlichen Applikationen integriert sein
- Die Anwendung muss benutzerfreundlich und effizient sein
- Microsoft RMS unterstützt Office-Palette
 - Sehr gute Integration
 - Development Kit verfügbar
 - Siehe Vortrag Armand Portmann
- Adobe schützt PDF-Dokumente
 - Sehr gute Integration auch in Adobe Reader

Anforderung 6: Übertragung von Rechten

- Bei jeder Firma gibt es Personalmutationen
- Die Rechte sollten bei Personalmutationen dynamisch geändert oder an andere Personen übertragen werden können
- Als Minimum muss die Revokation von Rechten möglich sein

Anforderung 7: Nachträgliches Ändern von Rechten

- Die Berechtigungen müssen nach der Verteilung der Dokumente geändert werden können
- Zugriff für weitere Personen
- Konkrete Berechtigung für eine Person muss angepasst werden können (z.B. Druckrechte)

Anforderung 8: Monitoring des Zugriffs

- Alle erfolgten Zugriffe sollten nachvollzogen werden können
 - SOX lässt grüssen
 - Zugriff zu ungewöhnlichen Zeiten deuten auf Missbrauch hin
- Eventuell Probleme bei Offline-Anwendungen

Anforderung 9: Offline Gebrauch

- Es soll ein Zugriff auch ohne unmittelbaren Zugriff auf den Lizenzserver möglich sein
- Beeinträchtigt Monitoring und Tracking
- Ein Revozieren von Berechtigungen ist nicht garantiert
 - Problem bei entlassenen Mitarbeitern

Anforderung 10: Einfache Identifikation

- Die Identifikation der Teilnehmer muss einfach sein
 - Wer hat das Dokument erstellt?
 - Wer hat Zugriffe auf das Dokument?
 - Wem gebe ich Zugriff auf das Dokument?
- Die email-Adresse eignet sich gut dafür

Anforderung 11: einfache Verifikation

- Das Dokument muss verifizierbar sein
 - Wer hat das Dokument erstellt?
 - Ist die Integrität sichergestellt?

Vergleich von verschiedenen Systemen

	Requirement	RMS	Authentica	Adobe
01	Persistent Protections	3	3	3
02	Inter-company transactions	1	2	3
03	Portability: Time Shifting	3	3	3
04	Portability: Space Shifting	2	3	2
05	Portability: Format Shifting	2	1	0
06	Portability: Platform Shifting	0	0	3
07	Excerpting	3	3	3
08	Integration with existing applications	2	0	1
09	Transfer of Rights	2	3	1
10	Allow for changes to access and usage rights after distribution	0	3	3
11	Track usage of DRM works	3	3	2
12	Offline Usage	3	-	3
13	Easy identification	2	2	3
14	Easy Verification	3	3	3
	Total (out of 42 assuming equal weighting)	29	29	33

Zusammenfassung

- Es wird immer schwieriger mit klassischen Zugriffssystemen die Informationen zu schützen
 - Die Kryptologie wird in Zukunft eine grosse Rolle spielen
- Anforderungen an ERM-Systeme können widersprüchlich sein
 - Grosse Unterschiede bei den erhältlichen Produkten
 - Es gibt nicht das beste Produkt!
- Management Prozesse können komplex sein
- ERM-Systeme lösen nicht alle Probleme
 - Es gibt Probleme, die ohne ERM nicht gelöst werden können