

# Löschen im Internet

Erhebliche Diskrepanz zwischen Erwartung und Realität

Prof. Dr. Hannes Federrath

Universität Regensburg / Uni Hamburg (ab 1.4.11)

<http://www-sec.uni-regensburg.de>



Saarbrücken 22.2.11

## Schutzziele (Voydock, Kent 1983)

---

- Klassische IT-Sicherheit berücksichtigt im Wesentlichen Risiken, die durch *regelwidriges Verhalten* in IT-Systemen entstehen.

**Vertraulichkeit**

unbefugter Informationsgewinn

**Integrität**

unbefugte Modifikation

**Verfügbarkeit**

unbefugte Beeinträchtigung der Funktionalität

## Vertraulichkeit

unbefugter Informationsgewinn

- Outsider
  - Betrachter des Inhalts
- Insider
  - Betreiber des Radiergummi-Systems (Schlüssel)
  - Betreiber des Speicher-Systems (geschützter Inhalt)

## Angreifermodell

---

Schutz vor einem allmächtigen Angreifer ist unmöglich.

Das Angreifermodell definiert die maximal berücksichtigte Stärke eines Angreifers, gegen den ein Schutzmechanismus gerade noch wirkt.

- Es beschreibt die

- Rollen des Angreifers (Insider, Outsider, ...)
- Verbreitung des Angreifers
- Verhalten des Angreifers
  - passiv / aktiv
- Rechenkapazität des Angreifers
  - unbeschränkt: informationstheoretisch
  - beschränkt: komplexitätstheoretisch

## Erreichbare Sicherheit

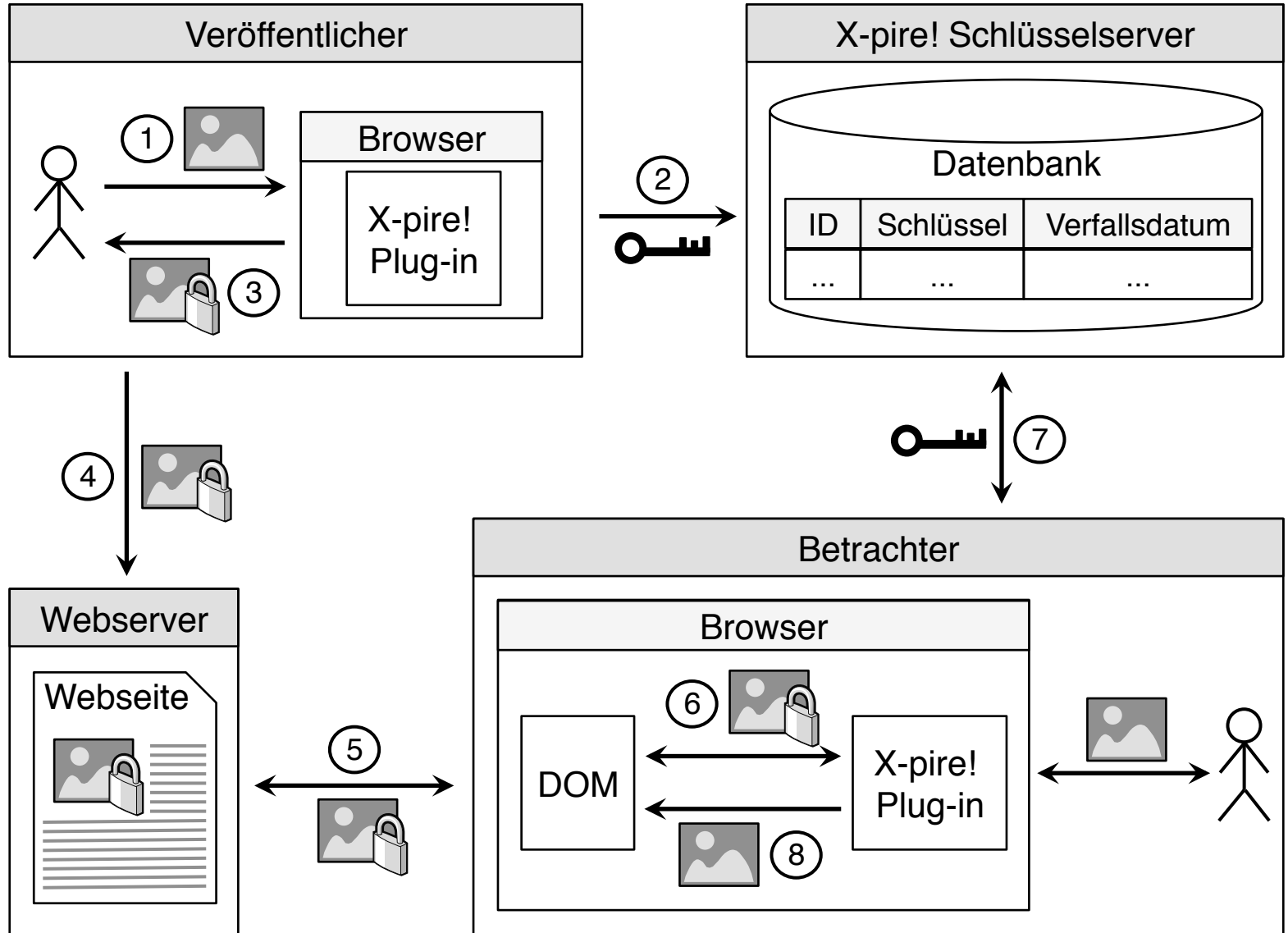
---

- (informations)theoretisch sicher
- (kryptographisch) stark (beweisbar)
  - » gegen aktive Angriffe
  - » gegen passive Angriffe
- wohluntersucht (praktisch sicher)
  - » Chaos
  - » Zahlentheorie
- [ geheim gehaltene ]

- unbedingt sicher
- perfekt sicher
- probabilistisch sicher
- ...

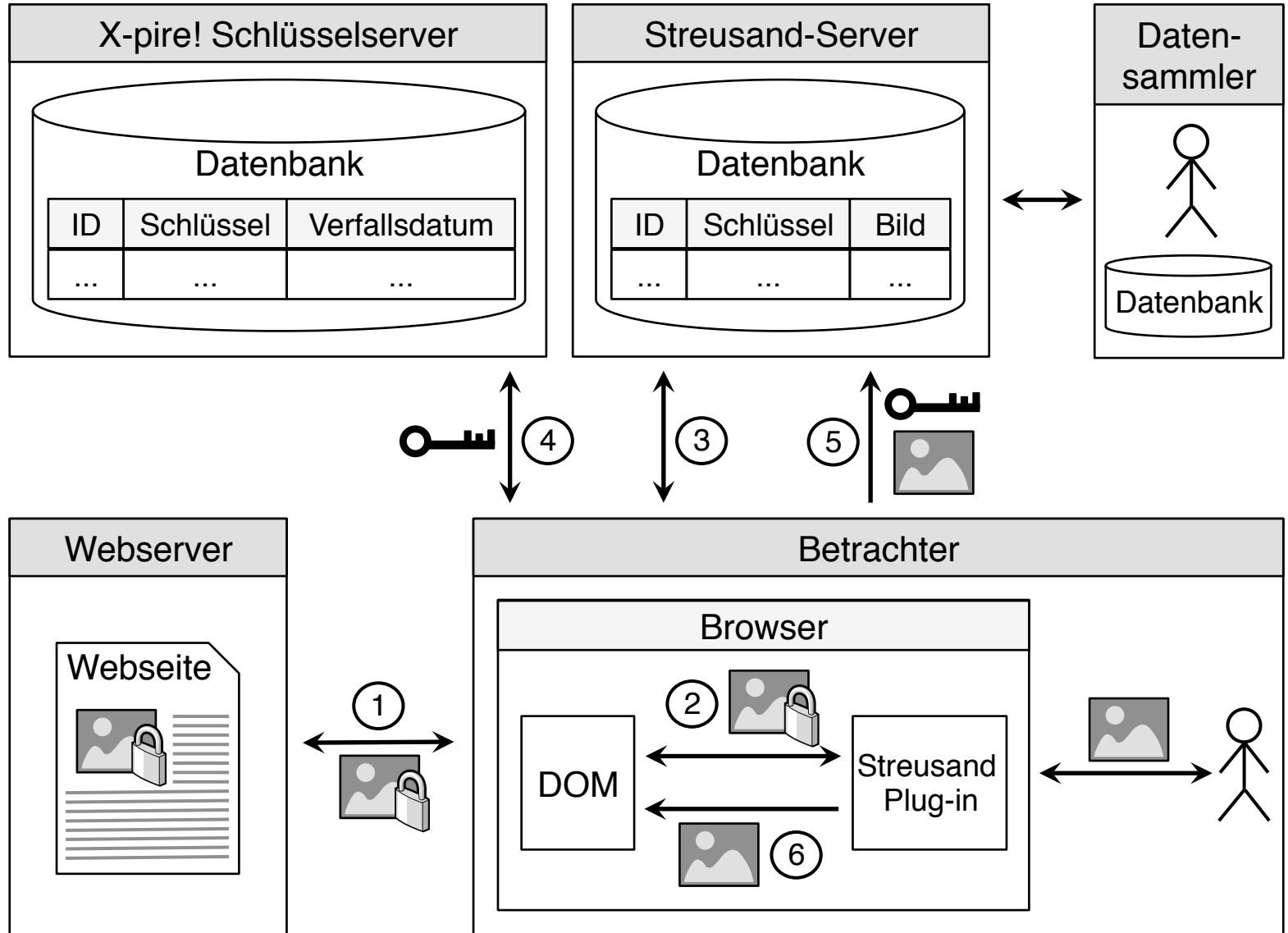
- Dies alles hat nahezu nichts mit der Aussage »100-prozentige Sicherheit gibt es nicht« zu tun!

# Funktionsweise X-pire!



- Zentraler Schlüsselservers
  - Verfügbarkeit: single-point-of-failure
  - Vertraulichkeit: Datenbank-Betreiber kennt alle Schlüssel
  - Erweiterungen denkbar:
    - Verteilte Datenbanken
    - Verwendung von Secret-Sharing-Verfahren und Anonymitätstechniken
- Kein Schutz gegen Angreifer in der Rolle »Betrachter«
  - Software im Verfügungsbereich des Betrachters (Browser) erhält Zugriff auf Schlüssel und unverschlüsselten Inhalt
    - Weder Verschlüsselung noch CAPTACHs helfen hier!
  - Streisand-Effekt

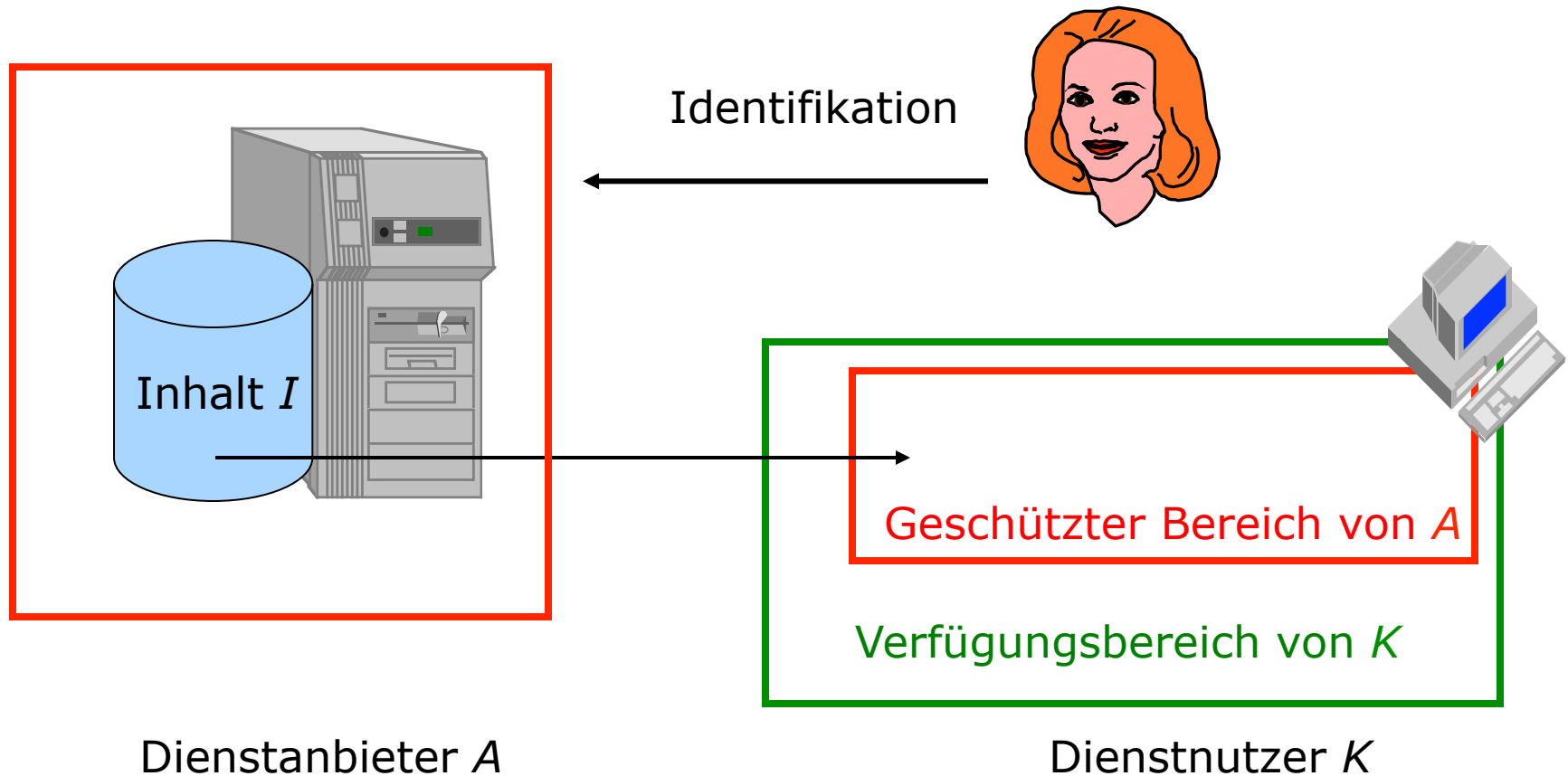
# Funktionsweise Streusand





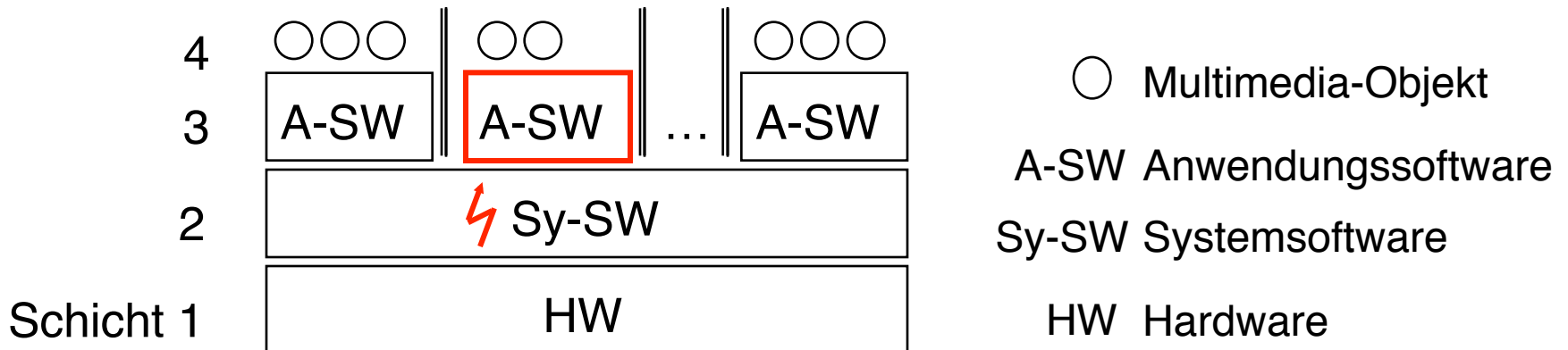
## Das DRM-Problem

- Einem Kunden  $K$  einen Inhalt  $I$  in einer bestimmten Weise zugänglich machen, ihm aber daran hindern, alles damit tun zu können.



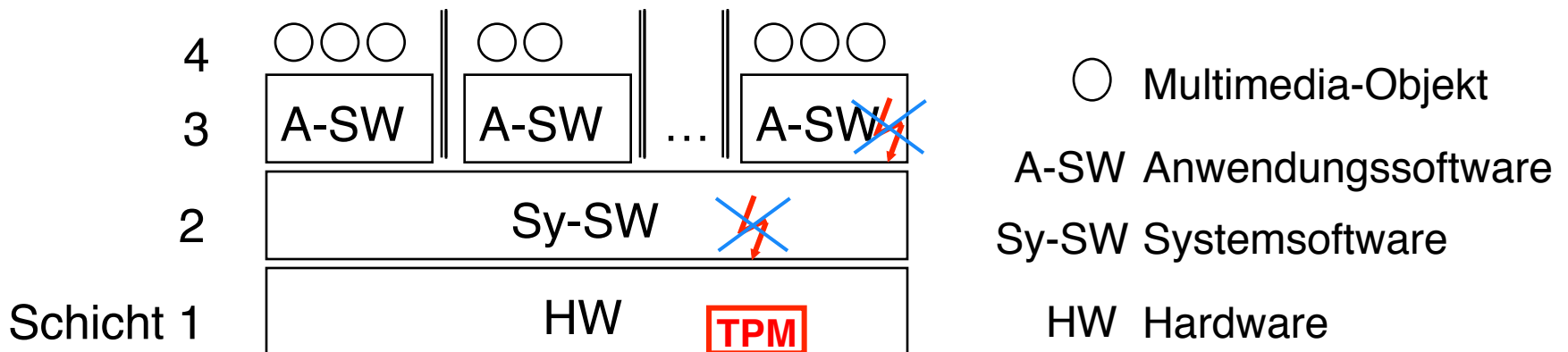
## Frei programmierbarer Universal-PC

- Ausführungs-Schichtenstruktur
  - Objekte können vor den darunter liegenden Schichten nicht effizient geschützt werden.
- Folge:
  - Auf frei programmieren PCs werden Multimedia-Objekte nie wirklich schützbar sein.



## [Nicht] Frei programmierbarer Universal-PC




- **Abwehr:**
  - spezielle Hardware (Tamper Proof Module, TPM), die im PC eingebaut ist
  - schützt vor Ausführung nicht autorisierter Programme
- **Folge:**
  - Es können nur noch offizielle Programme mit einem geschützten Inhalt verwendet werden.



## Schlussbemerkungen

- Demonstration der Grenzen des »Verfallsdatums«
  - keine Veröffentlichung der Software geplant
  - Programmieraufwand inkl. Reverse engineering
    - ca. 8 Stunden

- Nutzung kann schädlich sein
  - Streusand-Galerie
    - Bilder, die längst verschwunden sein sollten, existieren nun erst recht im Netz

01.02.2011 08:25:36	4d4d75d742863ab9656f5d576df858	a7385c51a134d53030ec2f18c7fcb689ad4094b06fb90e01c3abac722f1f5c	
31.01.2011 20:24:00	ab897fbdedfa502b2d839b6a56100887	cee65472de6234f647c5c25d959c2f116707f76eb7a5a54c2ad1a99e1d4628	
31.01.2011 20:23:12	ab897fbdedfa502b2d839b6a56100887	17150bb7b618f8e11358b5d8b7d6be438394213eb2a5c5f270348ee733c198e1	
31.01.2011 20:21:08	ab897fbdedfa502b2d839b6a56100887	2b4ce711793140ea5fa88c27f61354034f69dbbaae82f6c88490fc0d19bd09	
27.01.2011 18:29:03	e6f207509af3908da116ce61a757695	fb1cd38c912c46c41181c8eb32b39c396baacd60bf1d0683b6ca3d12ec386ba	

- Reine Softwarelösungen werden das Problem niemals lösen
  - Digital Rights Management war und wird nicht der Retter der Musik- und Filmindustrie sein.
  - Das digitale Verfallsdatum wird nicht dazu beitragen, die informationelle Selbstbestimmung der Bürger im Netz zu stärken.

Prof. Dr. Hannes Federrath  
Lehrstuhl Management der Informationssicherheit  
Universität Regensburg  
D-93040 Regensburg

E-Mail: [hannes.federrath@wiwi.uni-regensburg.de](mailto:hannes.federrath@wiwi.uni-regensburg.de)  
WWW: <http://www-sec.uni-regensburg.de>

Phone +49-941-943-2870  
Telefax +49-941-943-2888

