



# On Controlled Sharing of Virtual Goods

**Claudia Eckert, Frederic Stumpf**

Fraunhofer Institute for Secure Information Technology (SIT), Germany

**Omid Tafreschi**

Chair of Information Systems  
Technische Universität Darmstadt, Germany

Motivation

Trusted Computing

Attestation Protocols

A Fair Digital Rights Management System

Use Cases

System Architecture

Protocols

Conclusions

# Need for Digital Rights Management Systems



- ▶ Efficient compression algorithms and high bandwidths enable users to share digital content at low cost
  - ⇒ Emergence of file sharing and illegal usage

- ▶ Efficient compression algorithms and high bandwidths enable users to share digital content at low cost
  - ⇒ Emergence of file sharing and illegal usage
- ▶ Digital Rights Management Systems (DRMS) aim at controlling the usage of digital content
  - ▶ Definition of security policies (usage rules)
  - ▶ Enforcement of security policies

# Shortcomings of Current DRMS

- ▶ Protection measures of current DRMS rely on the basis of unreliable software-based solutions
  - ▶ Obscurity techniques are as long effective as long as the obscurity is undiscovered

- ▶ Protection measures of current DRMS rely on the basis of unreliable software-based solutions
  - ▶ Obscurity techniques are as long effective as long as the obscurity is undiscovered
- ▶ Current DRMS do not consider consumers' expectations
  - ▶ This may hamper the overall acceptance of DRM [Fet03]
  - ▶ According to [DSVW05], 75% of the consumers want to share music with others and would pay more for this kind of usage

- ▶ Protection measures of current DRMS rely on the basis of unreliable software-based solutions
  - ▶ Obscurity techniques are as long effective as long as the obscurity is undiscovered
- ▶ Current DRMS do not consider consumers' expectations
  - ▶ This may hamper the overall acceptance of DRM [Fet03]
  - ▶ According to [DSVW05], 75% of the consumers want to share music with others and would pay more for this kind of usage

⇒ A successful DRM system has

- ▶ to respect consumers' expectations and
- ▶ to provide reliable security mechanisms

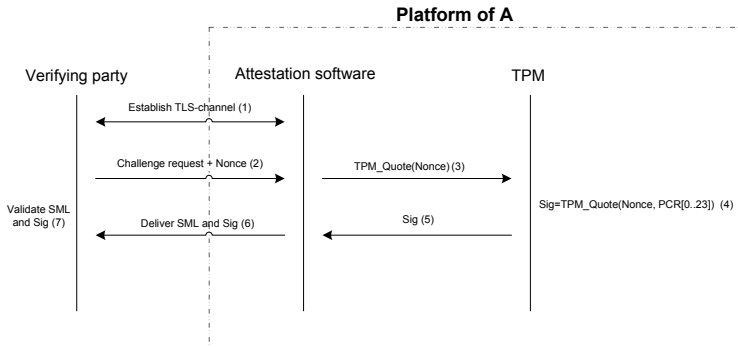
## Trusted Platform Module (TPM)

- ▶ Basically a smartcard
  - ▶ Protected storage of cryptographic keys
  - ▶ Possesses a number of special purpose keys (SRK, EK, AIK)
  - ▶ Hardware enhanced RNG, key generation, hash computation
- ▶ Platform Configuration Registers (PCR) to store software integrity values
- ▶ Binding a key to a specific sets of PCR (sealing)
- ▶ TPM acts as trust-anchor ⇒ Establishment of a *chain of trust*
- ▶ Attestation: Reporting the values of these registers to a remote entity using an *Attestation Identity Key* (AIK)





- ▶ Establishment of a TLS-channel
- ▶ Transfer attestation challenge
- ▶ Sending attestation response



# Masquerading Attack

- ▶ TCG-defined attestation process is insecure
- ▶ Attestation challenge can be relayed to another entity
- ▶ Enables a system to masquerade its own platform configuration
- ▶ Malware could exploit this characteristic to camouflage its presence



# Masquerading Attack

- ▶ TCG-defined attestation process is insecure
- ▶ Attestation challenge can be relayed to another entity
- ▶ Enables a system to masquerade its own platform configuration
- ▶ Malware could exploit this characteristic to camouflage its presence



- ▶ Shortcoming is caused by the restricted usage of *AIK*
  - ▶ Not possible to establish secure channels
  - ▶ Not usable for authentication of communication partners

# A Robust Integrity Reporting Protocol

## [STRE06]



TECHNISCHE  
UNIVERSITÄT  
DARMSTADT

- ▶ Malicious host must be excluded from communication
- ▶ Establishing a cryptographic link between both parties
- ▶ Cryptographic link must be established to the TPM
- ▶ *TPM\_Quote* allows injection of **external** data
- ▶ Use Diffie-Hellman key-exchange
- ▶ Inject  $g^s \bmod p$  into *AIK* signed message

# A Robust Integrity Reporting Protocol [STRE06]



- ▶ Malicious host must be excluded from communication
- ▶ Establishing a cryptographic link between both parties
- ▶ Cryptographic link must be established to the TPM
- ▶ *TPM\_Quote* allows injection of **external** data
- ▶ Use Diffie-Hellman key-exchange
- ▶ Inject  $g^s \bmod p$  into *AIK* signed message

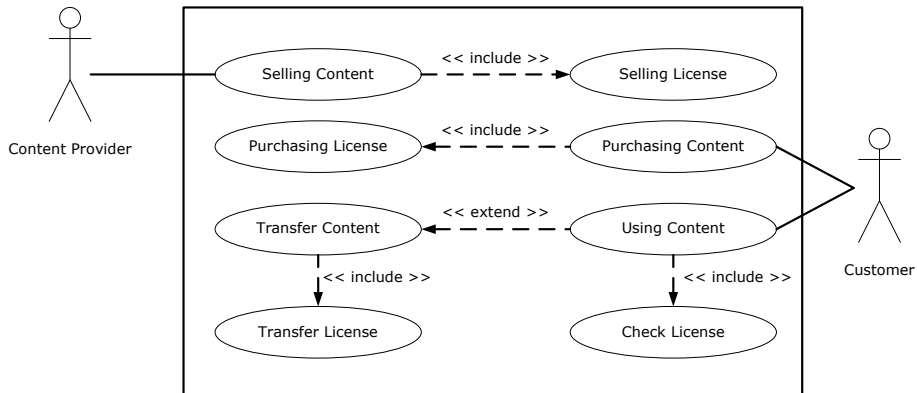
$$C \rightarrow S : Na, g^c \bmod p, g, p \quad (1)$$

$$C \leftarrow S : \text{Cert}(AIK, K_{AIK}), \{g^s \bmod p, Na, PCR\}_{K_{AIK}^{-1}} \quad (2)$$

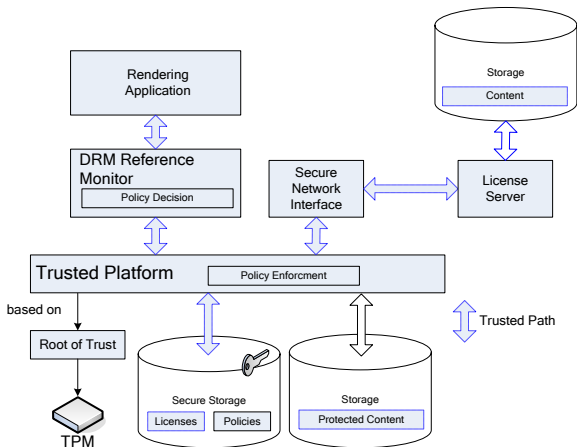
$$C \rightarrow S : \{Nb, g^c \bmod p\}_{K_{session}} \quad (3)$$

$$C \leftarrow S : \{Nb, Na, SML, g^s \bmod p\}_{K_{session}} \quad (4)$$

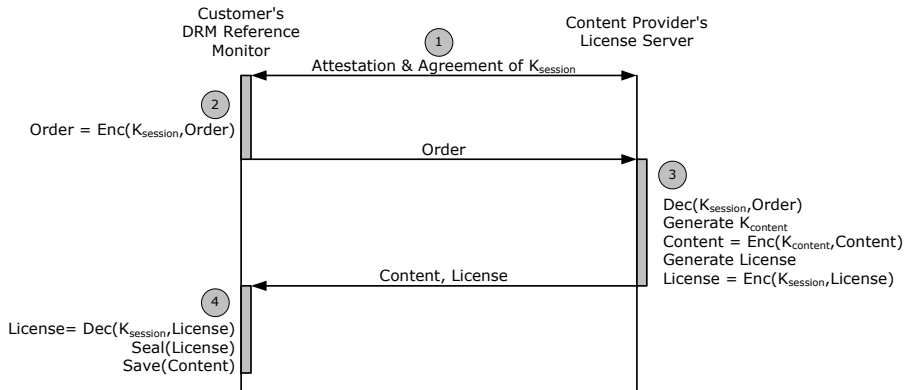
# Fair DRMS - Use Cases



# Fair DRMS - System Architecture

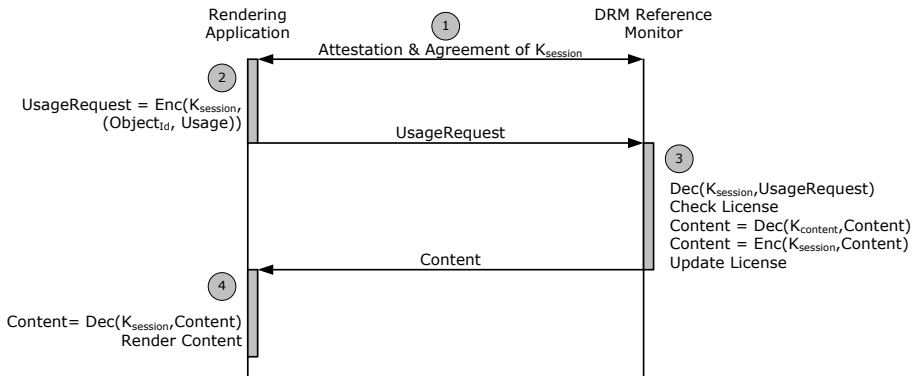


# Fair DRMS - Purchasing Content

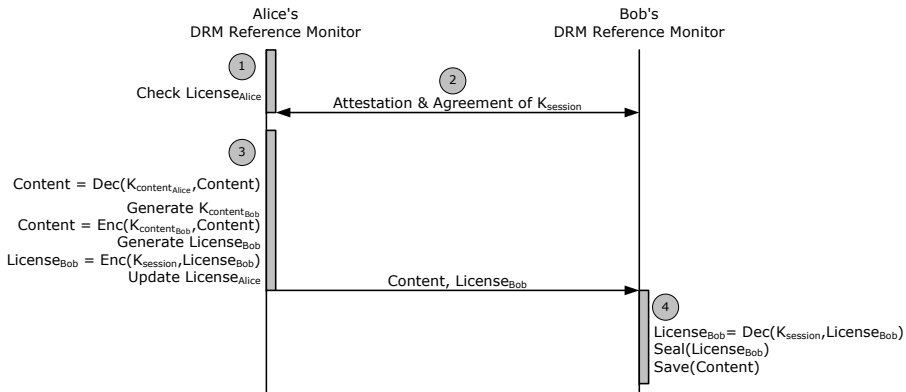




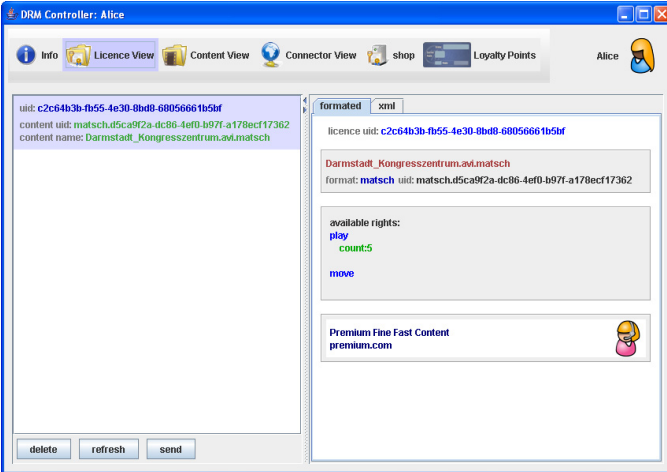
# Fair DRMS - Using Content



# Fair DRMS - Transferring Content



# Fair DRMS - Prototype



The screenshot shows a web application window titled "DRM Controller: Alice". The interface includes a navigation bar with icons for "Info", "Licence View", "Content View", "Connector View", "shop", and "Loyalty Points". The user's name "Alice" and a profile icon are displayed in the top right corner.

The main content area is divided into two panels. The left panel displays the following information:

- uid: c2c64b3b-fb55-4e30-8bd8-68056661b5bf
- content uid: matsch.d5ca9f2a-dc86-4ef0-b97f-a178ecf17362
- content name: Darmstadt\_Kongresszentrum.avi.matsch

The right panel shows a detailed view of the licence, with tabs for "formatted" and "xml". The "formatted" view displays:

- licence uid: c2c64b3b-fb55-4e30-8bd8-68056661b5bf
- Darmstadt\_Kongresszentrum.avi.matsch**
- format: **matsch** uid: matsch.d5ca9f2a-dc86-4ef0-b97f-a178ecf17362

Below this, the "available rights:" section lists:

- play**
- count:5
- move**

At the bottom of the right panel, there is a section for "Premium Fine Fast Content" from "premium.com" with a small icon of a person wearing a yellow helmet.

At the bottom left of the interface, there are three buttons: "delete", "refresh", and "send".



- ▶ Successful DRMS have to
  - ▶ be robust and
  - ▶ consider customers' expectations



- ▶ Successful DRMS have to
  - ▶ be robust and
  - ▶ consider customers' expectations
- ▶ Trusted computing can provide the necessary foundation
  - ▶ Hardware-based DRMS
  - ▶ Interoperable DRMS

- ▶ Successful DRMS have to
  - ▶ be robust and
  - ▶ consider customers' expectations
- ▶ Trusted computing can provide the necessary foundation
  - ▶ Hardware-based DRMS
  - ▶ Interoperable DRMS
- ▶ TCG-defined integrity reporting is vulnerable to masquerading attacks
- ▶ Proposed integrity reporting protocol prevents masquerading attacks

- ▶ Successful DRMS have to
  - ▶ be robust and
  - ▶ consider customers' expectations
- ▶ Trusted computing can provide the necessary foundation
  - ▶ Hardware-based DRMS
  - ▶ Interoperable DRMS
- ▶ TCG-defined integrity reporting is vulnerable to masquerading attacks
- ▶ Proposed integrity reporting protocol prevents masquerading attacks
- ▶ Presented DRMS enable customers to transfer their content to other customers or devices

Thank you for your attention  
Any Questions?







N. Dufft, A. Stiehler, D. Vogeley, and T. Wichmann.

Digital Music Usage and DRM - Results from an European Consumer Survey, May 2005.



M. Fetscherin.

Evaluating Consumer Acceptance for Protected Digital Content.

In E. Becker, W. Buhse, D. Günnewig, and N. Rump, editors, *Digital Rights Management*, volume 2770 of *Lecture Notes in Computer Science*, pages 321–333. Springer-Verlag, 2003.



F. Stumpf, O. Tafreschi, P. Röder, and C. Eckert.

A Robust Integrity Reporting Protocol for Remote Attestation.

In *Second Workshop on Advances in Trusted Computing (WATC'06 Fall)*, November 2006.