

# Fraunhofer Institute for Digital Media Technology IDMT

---

Traceability and Privacy:  
The Separation of Duty Approach of the  
LWDRM (Lightweight DRM) System

---

Patrick Aichroth

*ath@idmt.fraunhofer.de*

---

# Overview

- Introduction to Lightweight DRM (LWDRM)
  - Basic Idea, Features
  - Mp3p and LWDRM export
  - Certification and architecture overview
- Traceability vs. Privacy: “Separation of Duty“
  - Main problems and requirements
  - Impact on data formats and architecture
  - Conclusion

---

## Introduction to LWDRM: Basic Idea

- Allows copying if the consumer is willing to sign content, i.e. mark it with his identity (results in a Signed Media File, or SMF).
- Content can be transferred/rendered without restrictions within the personal environment
- Content can be traced back to the consumer in case of illegal public dissemination
- Meets the demands of content providers and consumers at the same time

---

# Introduction to LWDRM: Features

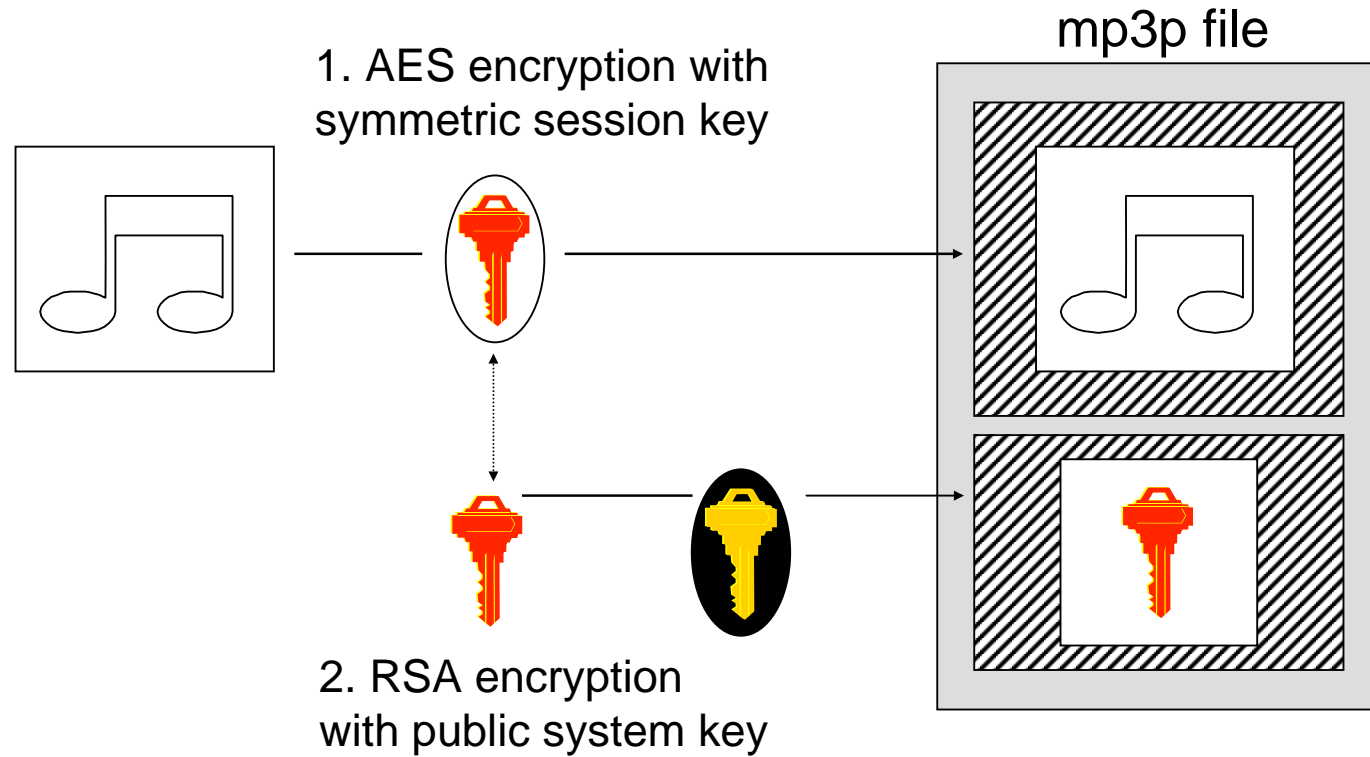
- Based on traceability (no copy protection)
- Uses cryptographic means and digital watermarks as a „second line of defense“
- ISO media file format
- MPEG-4, RSA, AES, ISMACryp

---

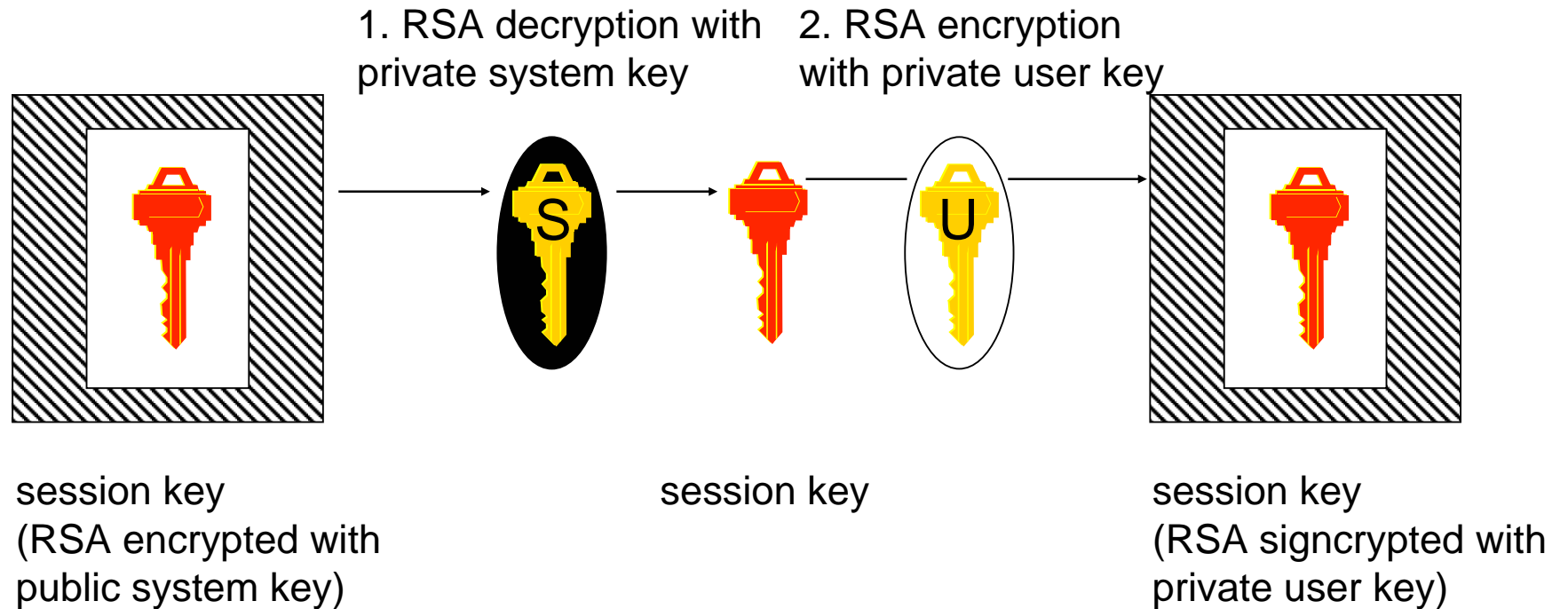
# Introduction to LWDRM: mp3p and LWDRM

- Current Implementation: LWDRM is an add-on to the mp3p (mp3 protected) DRM system:
- Content is initially copy-protected (bound to a target system) using the mp3p system. Usage restrictions/limitations apply!
- LWDRM add-on: „SMF export“ option - a user can always choose to generate signed content, and get rid of usage restrictions/limitations.

# Introduction to LWDRM: Secure delivery (mp3p file generation)



# Introduction to LWDRM: SMF export (mp3p to SMF conversion)

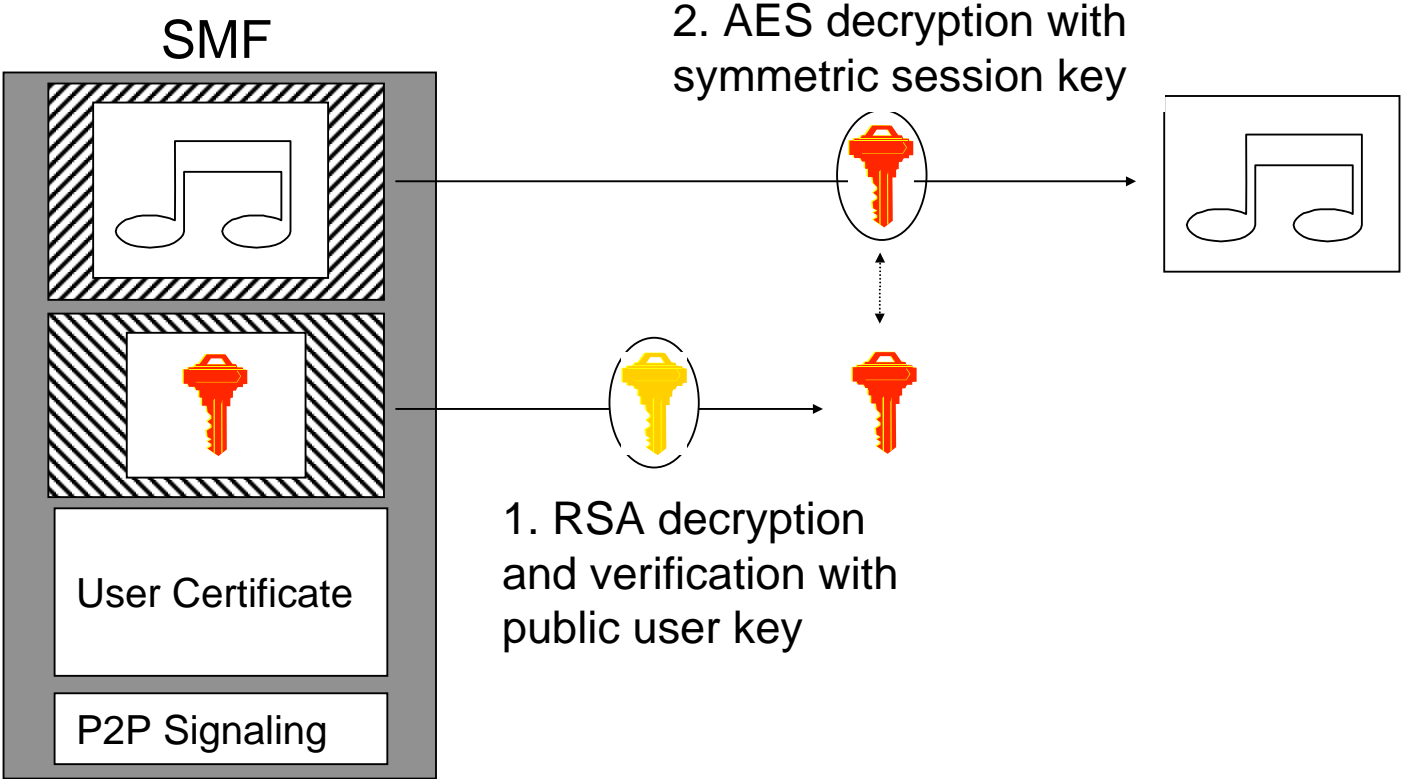


---

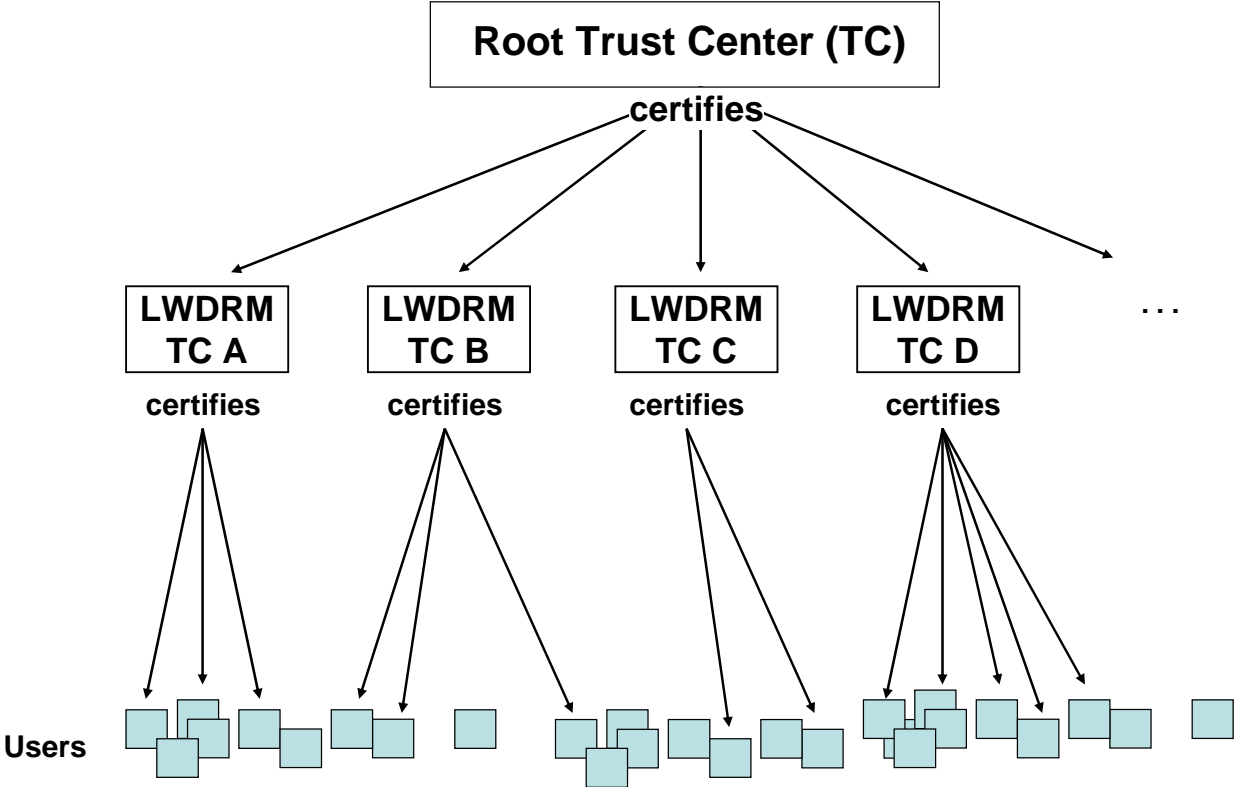
# Introduction to LWDRM: Signed Media File (SMF)

- Encryption with private user key („signcrypton“)
- Contains user certificate (and with it the user public key!)
- Unrestricted playback on all LWDRM compatible devices
- SMF playback is easy to implement
- User certificates are issued by LWDRM Trust Centers

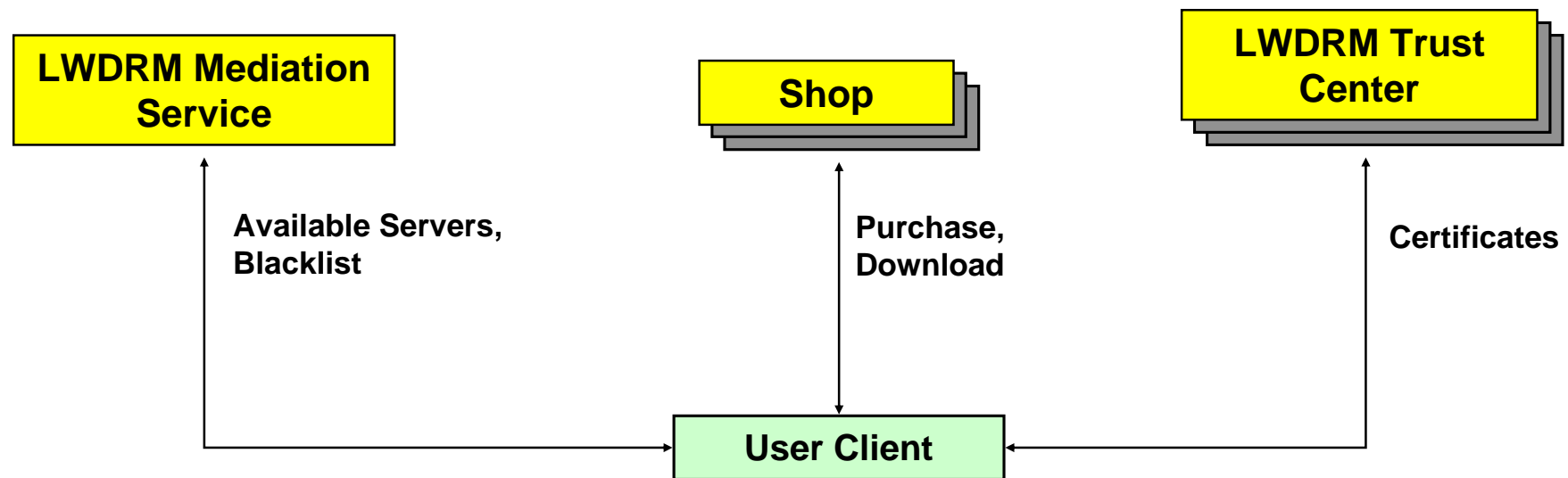
# Introduction to LWDRM: Signed Media File (SMF) playback



# Introduction to LWDRM: 2-layer certification hierarchy



# Introduction to LWDRM: Architecture (overview)



---

# Traceability vs. Privacy: Conflict of interest

- User interest: privacy and confidentiality of user data (fear of misuse, e.g. spamming by third parties, arbitrary tracing and persecution scenarios...)
- Content provider interest: means for resolving the identity of users
- A possible solution: the „Separation of Duty“ approach

---

# Traceability vs. Privacy: Requirements

1. Signed Media Files (and user certificates) must not contain any personal user data
2. Digital watermarks must not contain any personal user data
3. System architecture and data formats have to be designed in such a way that shops do not obtain the user id's used for user certificates and digital watermarks (assumption: shops do know their customers)

---

# Traceability vs. Privacy: Impact on data formats and architecture

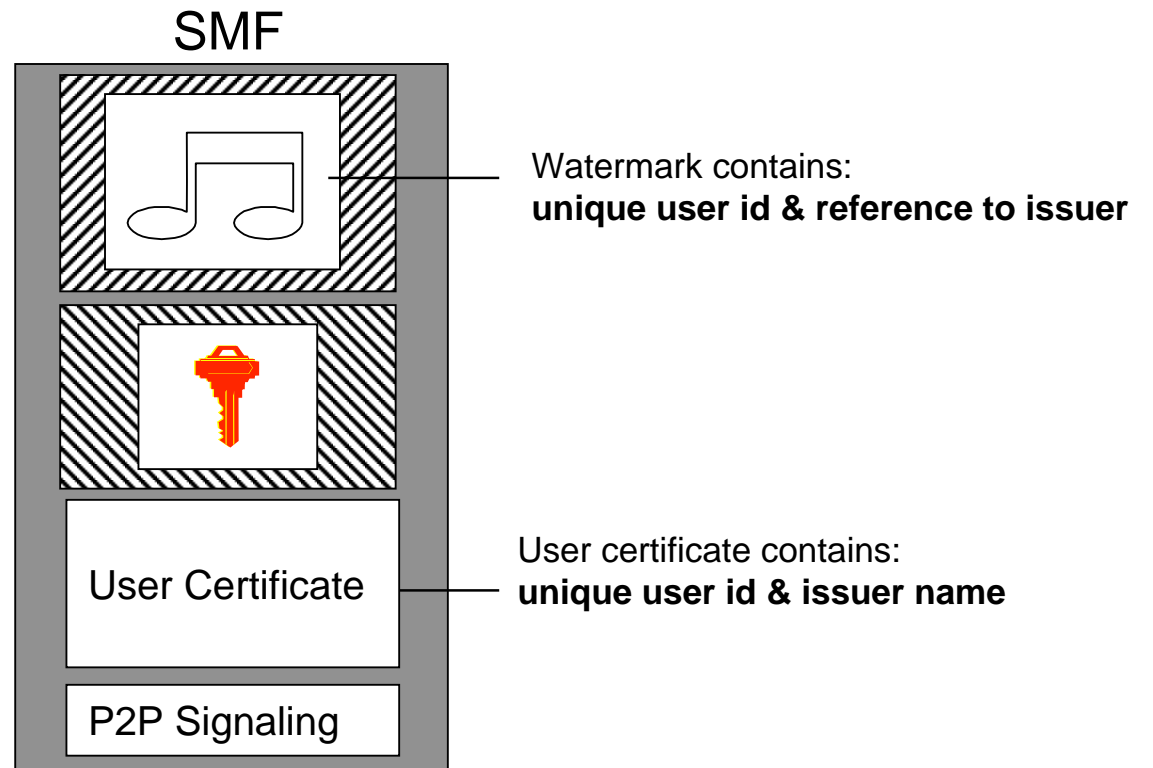
1. Signed Media Files (and user certificates) must not contain any personal user data
  - Use of pseudonymized certificates: User certificates contain a unique user id, and a reference to the issuing trust center
  - Only the Trust Center that has issued a certificate is able to reveal the personal data to a given user id
2. Digital watermarks must not contain any personal user data
  - Watermarks contain a unique user id, and a reference to the issuing trust center

---

# Traceability vs. Privacy: Impact on data formats and architecture

3. System architecture and data formats have to be designed in such a way that shops do not obtain the user id's used for user certificates and digital watermarks
  - Communication between client and Trust Center is totally independent from client-shop communication. User id's are not used for client-shop communication
  - Signing and watermark embedding take place on the client side
  - No transactional data is being embedded within a Signed Media File in order to prevent shops from revealing the user's real identity

# Traceability vs. Privacy: Impact on data formats and architecture



SMF contains **no user or transactional data**

---

# Traceability vs. Privacy: Conclusion

- Main problem: Many users do not trust in that content providers will always stick to legal guidelines
- “Separation of Duty”: Only a Trust Center can reveal the personal data to a given user id, and it will do so only when legal directives are there
- It is not up to DRM technology to decide what is legal, and what is not. With the proposed approach, LWDRM tries to leave that question to those responsible for it