

# ***How to Increase the Security of Digital Rights Management Systems without Affecting Consumer's Security***



4FriendsOnly.com  
Internet Technologies AG

**PD Dr.-Ing. habil. Jürgen Nützel,  
CEO, JN@4FO.de  
4FriendsOnly.com AG**



TECHNISCHE  
UNIVERSITÄT  
ILMENAU

**Anja Beyer  
Anja.Beyer@tu-ilmenau.de  
Technische Universität Ilmenau**



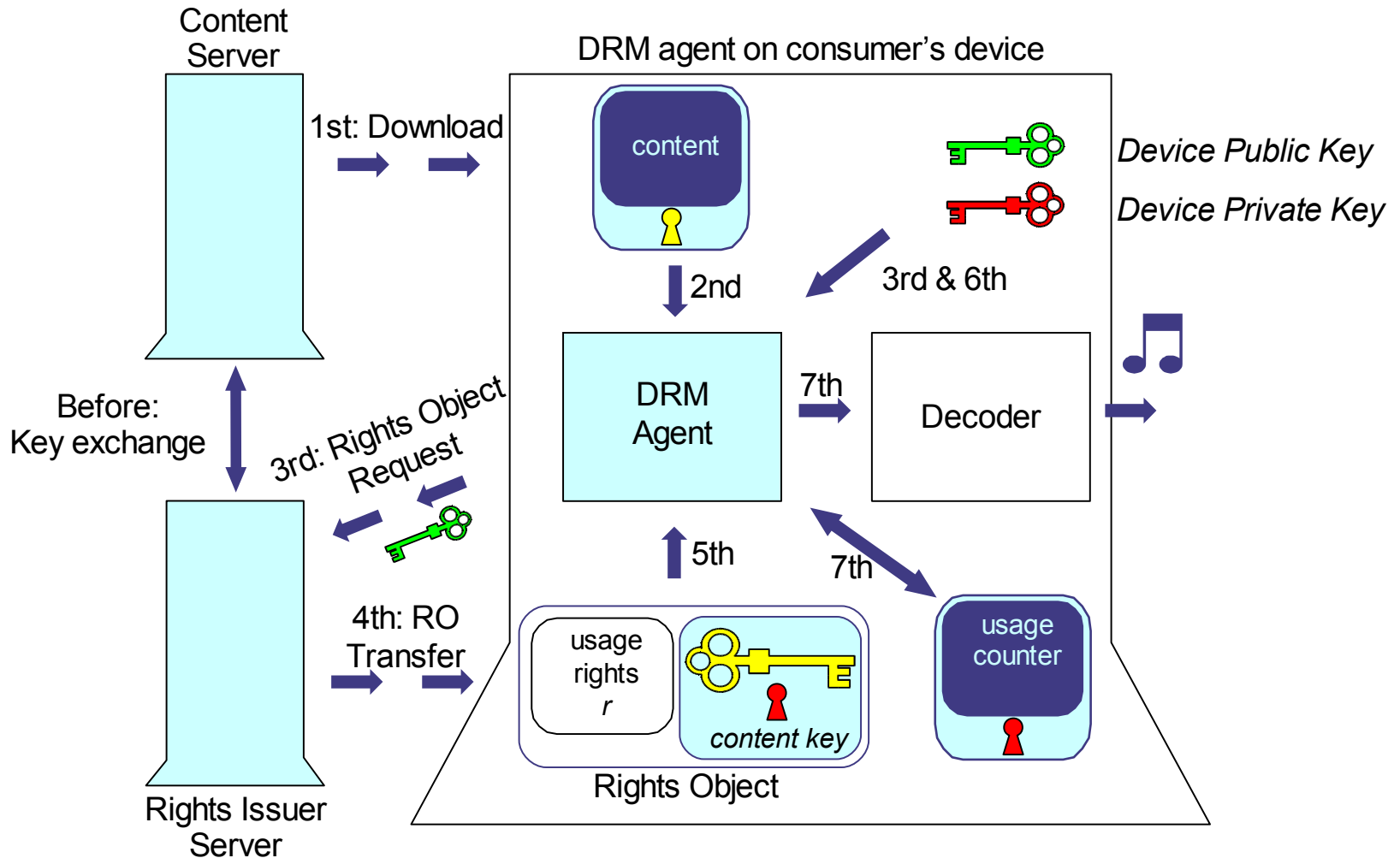
# Outline

- ❑ **Digital Rights Management (DRM)**
- ❑ **Security Aspects for DRM Systems**
  - *The Competition of Provider's and User's Security*
- ❑ **Open Mobile Alliance (OMA) DRM**
  - *What is OMA?*
  - *Trust and Security Model of OMA DRM Version 2*
- ❑ **Obfuscation of OMA DRM (Version 2) Agents**
  - *Obfuscation of the Key Store*
  - *Hidden Key Download*
- ❑ **Conclusions and Further Work**

# ***Digital Rights Management (DRM)***

- ❑ Duplicating virtual goods (like music) is cheap**
- ❑ DRM was established to control users' copying**
- ❑ Now DRM is more than only copy protection**
- ❑ No standardized definition for DRM**
  - *... procedures that help to protect the rights of the virtual goods in a way that we are accustomed from the intellectual products bound to physical media.***
  - *Copy and transfer shall be linked to the rules of the rights holder, thus the content provider***

# DRM Architecture (OMA)



# Security Aspects for DRM Systems

## □ Competition of Provider's and User's Security

- *The content is the most valuable asset of the provider*
- *A stable system is the most valuable asset of the user*

	Content provider	User
Asset	Content	System
Objectives	Confidentiality (protection against unauthorised usage of licenses)	Integrity of the system (hardware and software)
Threat	Extraction of the private decryption/license key	Loss of integrity of the system

## □ Therefore content providers should rely on ...

- *Open standards and*
- *their correct implementations*

# Open Mobile Alliance (OMA) DRM

## □ The only open and wide-spread DRM standard

- *„OMA is the leading industry forum for developing market driven, interoperable mobile service enablers“*
- *[www.openmobilealliance.org](http://www.openmobilealliance.org)*



## □ OMA DRM 1.0

- *Simple format independent DRM standard*
- *Supported by many mobile devices*
- *Supports: forward lock, combined and separated delivery of the key*

## □ OMA DRM 2.0

- *Standard was approved in March 2006*
- *Is not limited to mobile devices*
- *Nokia released its first device with OMA DRM 2.0*

Nokia N91



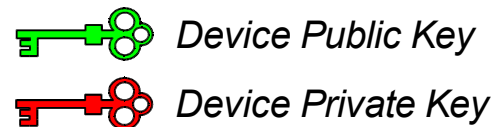
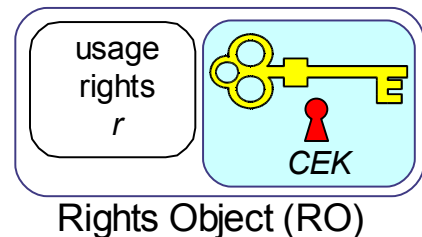
# Trust and Security Model of OMA DRM 2

## □ Device authentication based on ...

- ... X.509v3 certificates (*Device Certificates*)
- Certificates issued by a specific OMA CA
- Device private key is stored hidden/secure in the client device

## □ Rights Issuer uses ...

- ... the device public key (in certificate) to encrypt the Content Encryption Key (CEK) in the Rights Objects (RO)
- RO's only work on the device with the appropriate private key



- Device private key has to be kept secure

# *Two major problems we had to solve*

## **Secure storage of the device private key**

- *No secure storage on a PC platform*
- *We use platform specific hardware parameters*
- *We do not want to modify the operating system*

## **Installation of the device private key**

- *PC platforms have no preinstalled OMA device private key*
- *OMA standard has no answer for this problem*

## **Today we can not rely on Trusted Computing**

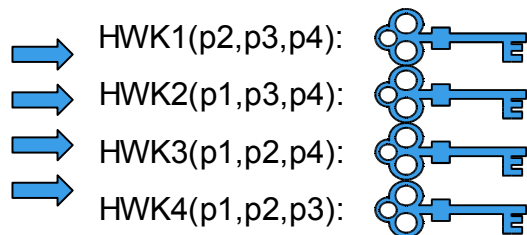
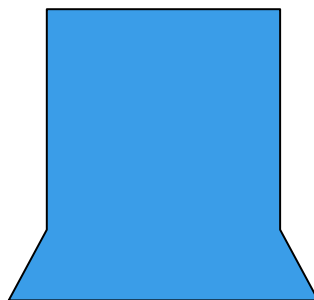
- *Not yet supported by operating systems*
- *PC boards with TPM not widely spread*

# Obfuscation of the Key Store

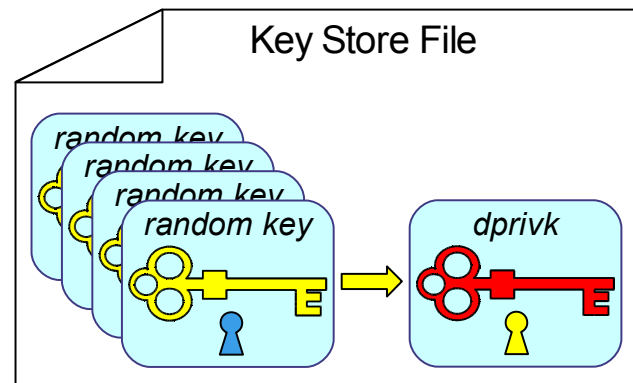
## Implementation for PC based platform

### Device private key encrypted with hardware parameters

Client Device with  
(n=4) different hardware  
parameters: p1,p2,p3,p4



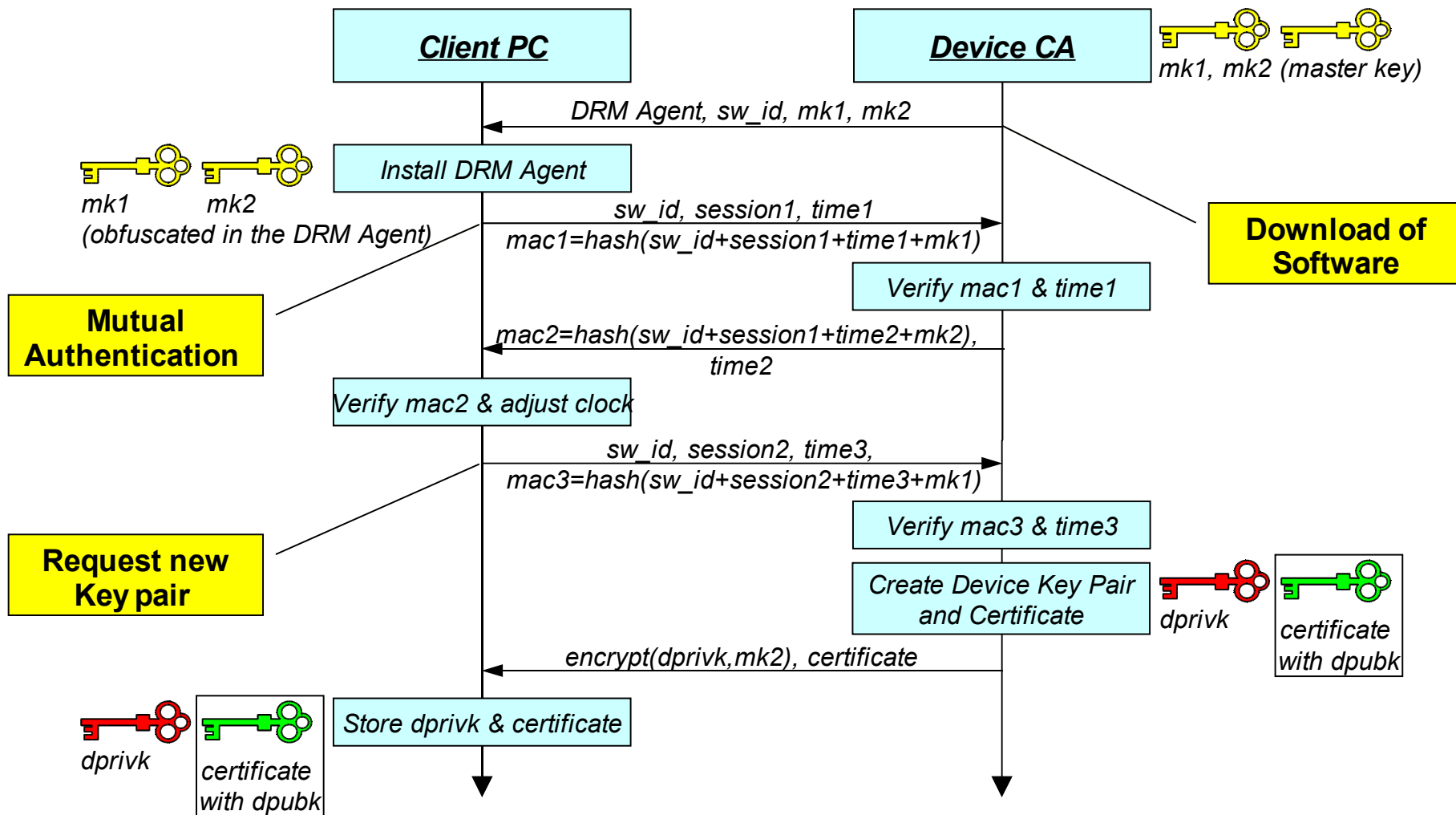
4 different hardware keys  
(HWK) are derived from 4 different  
subsets of the hardware parameters



The random key (RK) Device Private Key  
is encrypted 4 times

- In the implementation for Fraunhofer IIS eight hardware parameters (MAC, graphic card ...) are used
- Two hardware parameters may fail
- Random key is encrypted 56 times

# Hidden Key Download



# ***Conclusions and Further Work***

- ❑ Secure implementation of DRM without effecting users' security**
- ❑ Open standards as advantage for the users**
- ❑ Device private key is the security anchor of the DRM system**
- ❑ A hidden distribution of the device private key is still necessary**
- ❑ Using Trusted Computing Group's TPM**
  - *TPM (Trusted Platform Module) creates device certificates***
  - *TPM sends public key with a certificate request to the OMA device CA***
  - *Private key is bound to TPM***

# *Many thanks to*



**Fraunhofer**  
Institut  
Integrierte Schaltungen



**4FriendsOnly.com**  
**Internet Technologies AG**



**TECHNISCHE  
UNIVERSITÄT  
ILMENAU**

**Jürgen Nützel and Anja Beyer**