May 2008

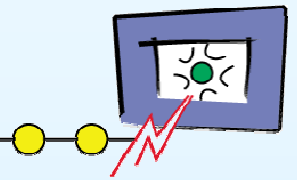
Content Protection Tools – ENTHRONE approach

ENTHRONE workshop, May 7, WIAMIS 2008
Klagenfurt University, Austria

Stefano Battista / bSoft
Itsik Arbel / Optibase

ENTHRONE
End-to-End QoS through Integrated Management of Content, Networks and Terminals
FP6 – 038463

ENTHRONE Content Protection (CP): Objectives

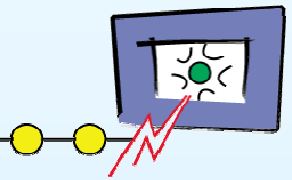


- Handle protected content, within an e2e QoS system, over the complete workflow – creation, delivery and consumption
- Show the value of MPEG-21 IPMP by introducing the concept of end-to-end security managed by EIMS, a high-level layer
- Provide the tools for this system
  - Including: encryption, license generation, rights evaluation and enforcement, cryptographic tools
- Support and contribute to DMP standardization
- Support for OMA BCAST 1.0 and DRM 2.0
- Interoperability
- Study of technologies for secure update of compromised DRM components within ENTHRONE terminal

Content Protection (CP) Framework

- **End-to-End Rights Management**
  - ENTHRONE Key Management System (KMS)
  - MPEG-21 REL (Rights Expression Language)
  - CP in Content Authoring Phase
  - CP Metadata Preparation
  - Content Protection TVM (CP-TVM)
  - License Server (LS)
  - Player and ISMACryp descrambling module
  - CP in content consumption phase
  - Remote update and secure renewability of IPMP Tools
- **Enable ENTHRONE e2e QoS management of protected content**
  - Restricted Adaptation
  - Cryptographic tools for scalable video

User Orientation

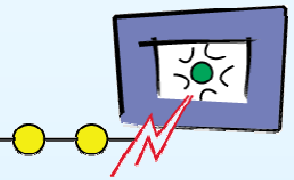


- Focus on the needs of the content consumer
  - End-user usability requirements
  - Unobtrusive, portable and ubiquitous CP
  - Restricted access to content-metadata
    - e.g., Blocking unauthorized access to adult content metadata
- Device interoperability
  - The Home Domain concept
  - Consuming licensed content in a variety of environments (home, mobile, etc.)
  - Content protection in scalable video consumption model
- Smart Card integration

Basic Functional Requirements

- **CP Business requirements**
  - Efficient use control
  - Motivating obedience
  - Law enforcing assistance
- **CP Technical requirements**
  - Security, Monitoring
  - Closing loopholes
  - Impersonation
  - Versatility
  - Accessibility
  - Non-Restrictiveness
  - Simplicity, Affordability
  - Privacy, Identification, Traceability

ENTHRONE CP in variety of content delivery scenarios



- **Broadcast TV and trans-scrambling**
- **VOD**
- **Content sharing and consumption within a Home Domain**
- **Subscription**
- **Content download from a web portal**
- **Sharing content with other Home Domains** (super-distribution and P2P)

DMP Compliance

- DMP provides a comprehensive ontology
- DMP is closely related to MPEG-21
- Supported DMP Requirements
  - Represent Content
  - Represent License
  - Represent Fixed DRM Tools
    - AES-CTR
  - Represent Fixed DRM Tools
  - Manage Domain
  - Represent License and Access License REL
  - Represent key information (Based on MPEG-21 REL)

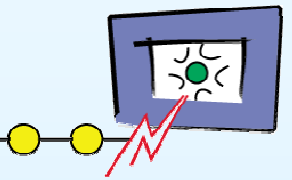
MPEG-21 IPMP + REL Compliance

- MPEG-21 IPMP is inclusive (including ISMACryp, for example, as a tool), but non-comprehensive
- Supported IPMP Requirements
  - Represent Content
  - Represent License
  - Represent Fixed DRM Tools
    - AES-CTR
  - Represent Fixed DRM Tools
  - Represent License and Access License REL
  - Represent key information (Based on MPEG-21 REL)
- Cryptographic tools for scalable video TVM
- Secure renewability of compromised IPMP tools

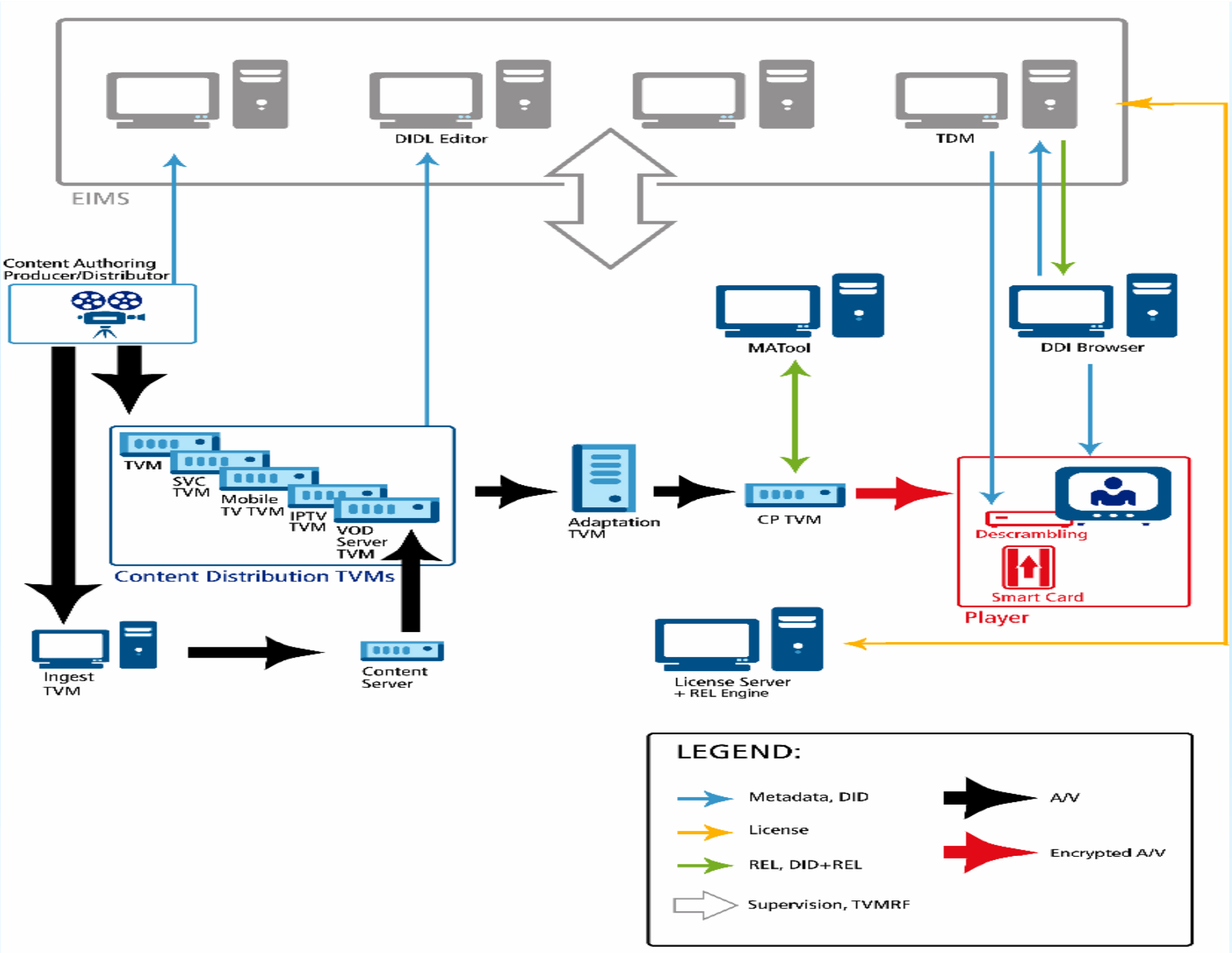
OMA Compliance

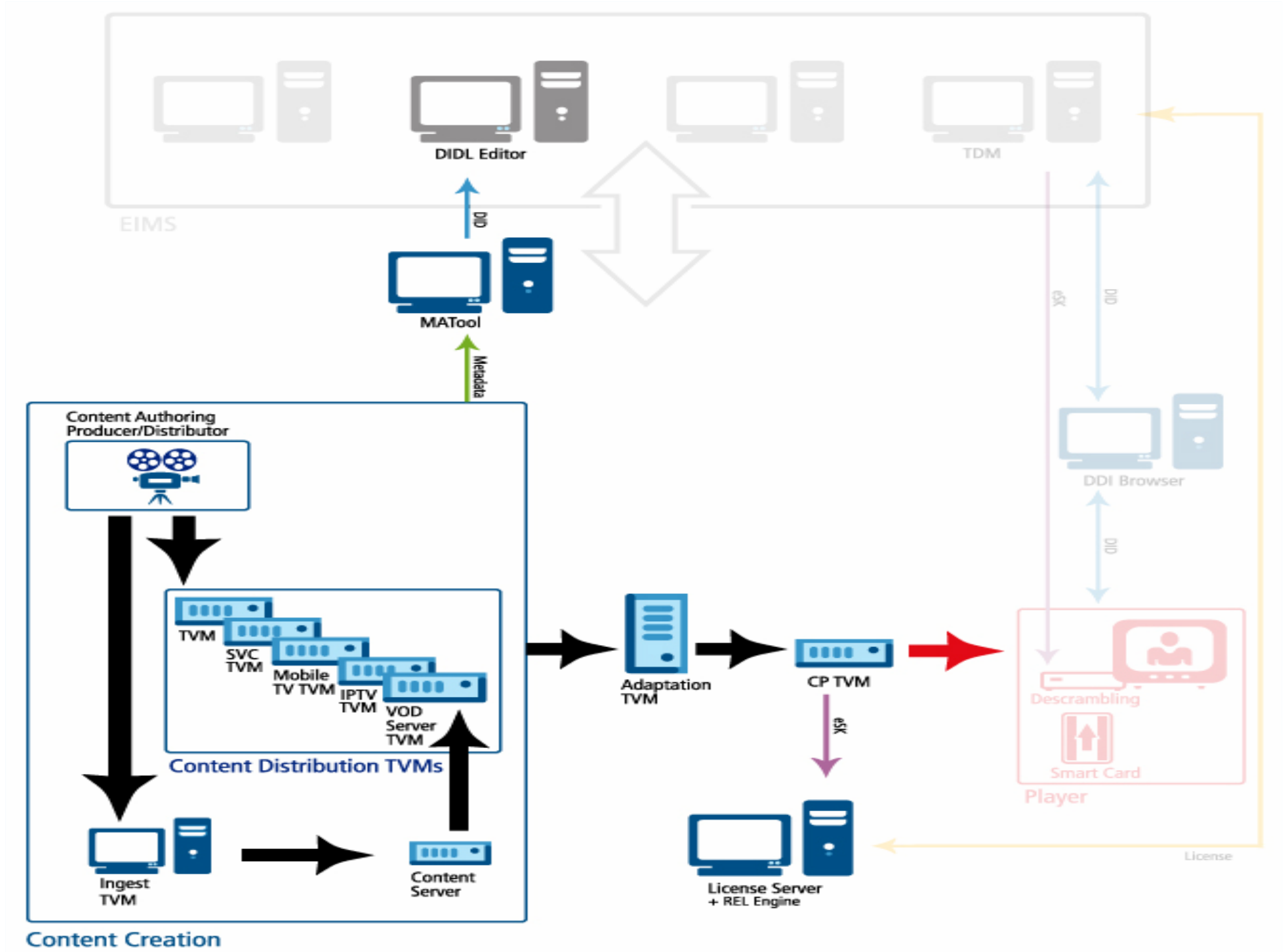
- OMA is inclusive (including ISMACryp, for example, as a tool), but non-comprehensive
- OMA licensing not as elaborate as MPEG-21 REL
- Supported OMA Requirements
  - Represent Content
  - Represent License
  - Represent Fixed DRM Tools
    - AES-CTR
  - Represent Fixed DRM Tools
  - Manage Domain
  - Represent License (ODRL, OMA-based MPEG-21 DTD)
  - Represent key information (Key Manager)
  - Authenticate servers and end-devices
- Support for OMA BCAST Service Protection SP 1.0
- Interoperability with MPEG-21 IPMP (limited functionality)

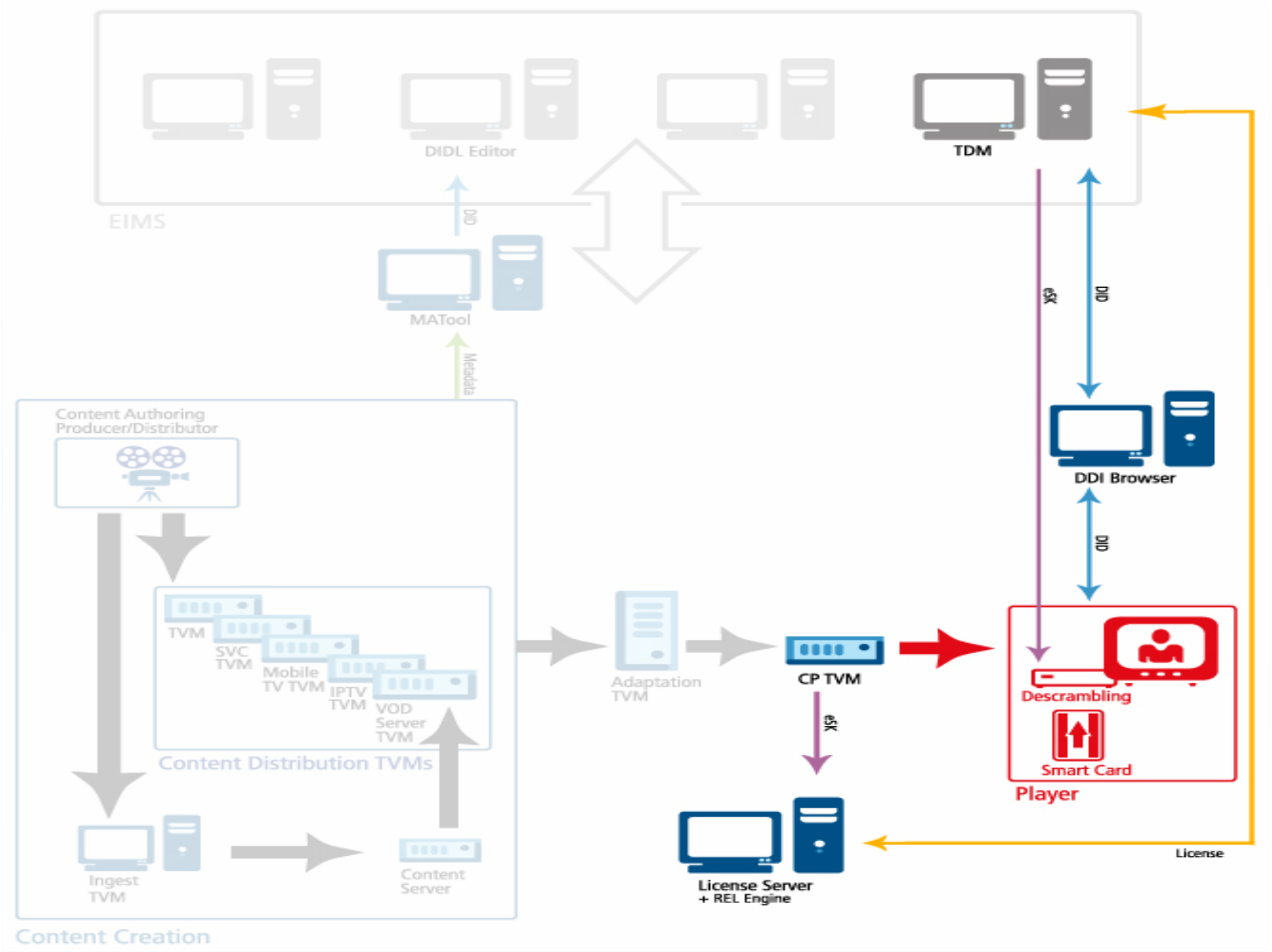
License Management



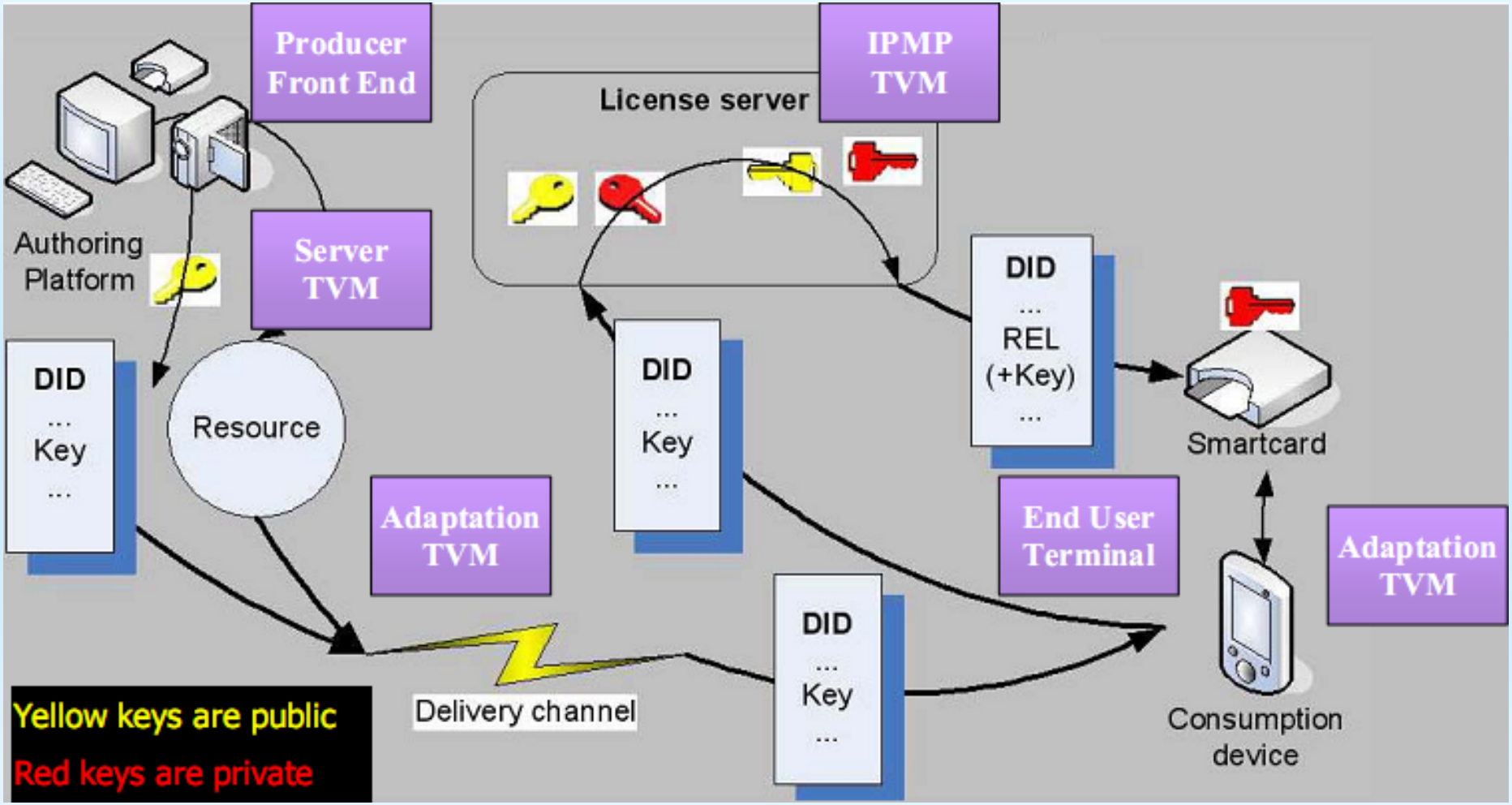
- ENTHRONE-II REL Schema
  - Adaptation-related REL Descriptors
- License Server (LS)
- REL Preparation and Handling
- REL authoring tool
- REL authentication tool


EIMS
DIDL Editor
TDM
Content Authoring
Producer/Distributor
MATool
DDI Browser
TVM
SVC TVM
Mobile TV TVM
IPTV TVM
VOD Server TVM
Content Distribution TVMs
Adaptation TVM
CP TVM
Descrambling
Smart Card
Player
Ingest TVM
Content Server
License Server + REL Engine
LEGEND:
Metadata, DID
License
REL, DID+REL
Supervision, TVMRF
A/V
Encrypted A/V


EIMS
DIDL Editor
TDM
DID
MATool
Metadata
Content Authoring
Producer/Distributor
TVM
SVC TVM
Mobile TV TVM
IPTV TVM
VOD Server TVM
Content Distribution TVMs
Ingest TVM
Content Server
Content Creation
Adaptation TVM
CP TVM
eSX
License Server + REL Engine
DDI Browser
DID
Descrambling
Smart Card
Player
License

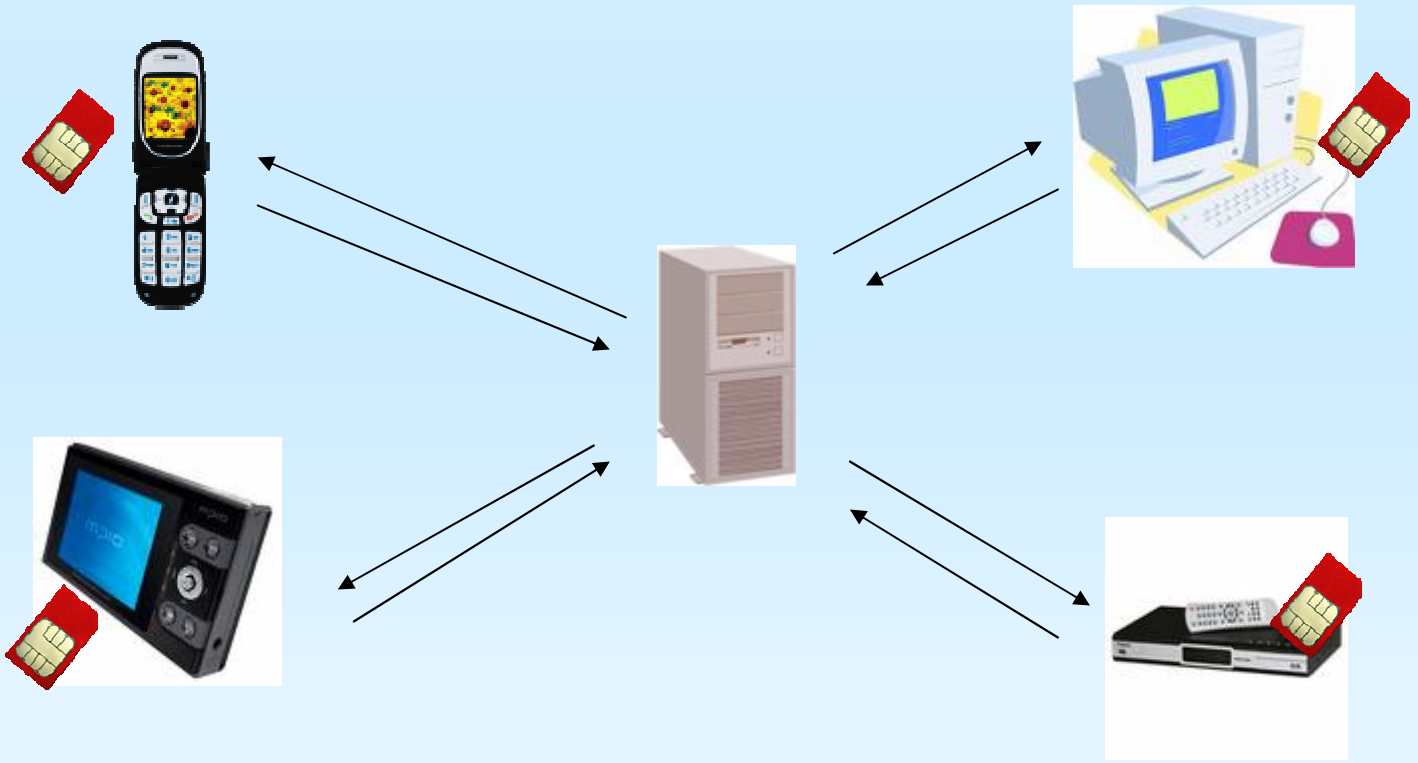

EIMS
DIDL Editor
TDM
DD
MATool
Metadata
esk
DID
DDI Browser
DID
Content Authoring
Producer/Distributor
TVM
SVC
TVM
Mobile
TV TVM
IPTV
TVM
VOD
Server
TVM
Content Distribution TVMs
Adaptation
TVM
CP TVM
esk
Descrambling
Smart Card
Player
Ingest
TVM
Content
Server
License Server
+ REL Engine
License
Content Creation

Key Management System (KMS)



Add a New Smart Card (SC) to a Home Domain (HmD)

- The SC requests the LS to join a Home Domain (HmD)
- The LS sends the private and public keys of the HmD and its public key to the SC.

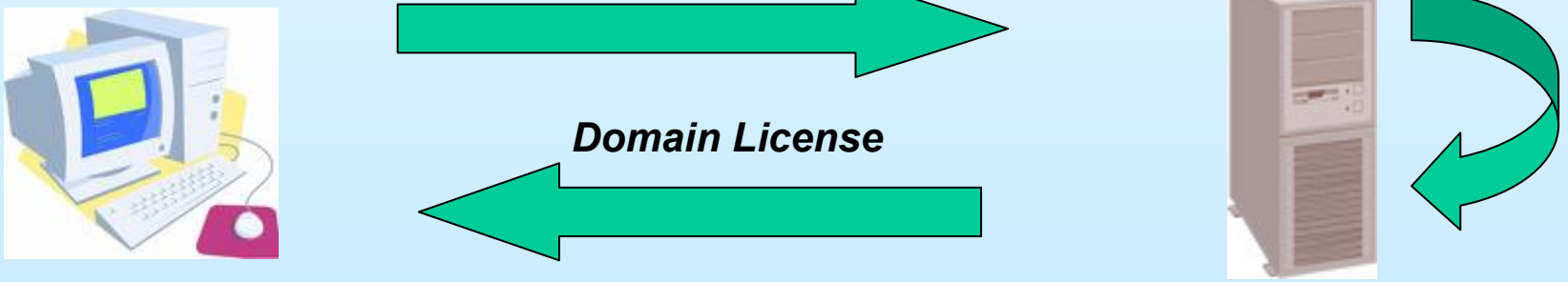


Acquire License Scenario 1

- The user receives the encrypted content and its *Sharing License*.

***Sharing License*,**
Encrypted Content

Acquire License Scenario 2 – Localization of the *Domain License*



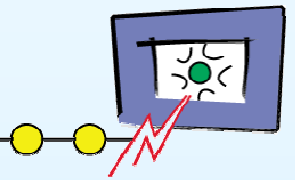
The user sends the *sharing license* and the HmD identifier to the LS

The LS:

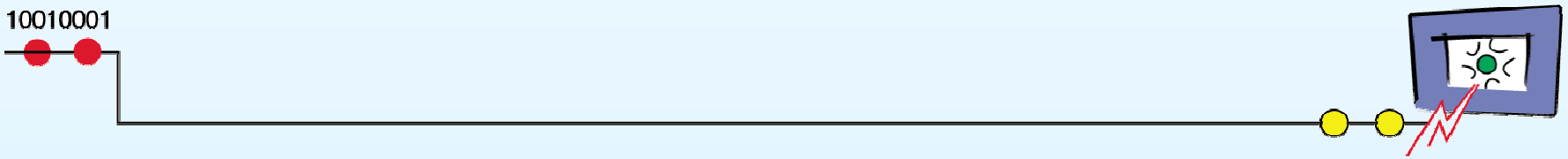
- Validates that the necessary financial transactions have been made.
- Transcribes the *sharing license*.
- Encrypts the scrambling key with the public key of the target HmD.
- Signs the transcribed DID (=*domain license*).

The *domain license* is sent to the user.

CP with content adaptation



- Content authoring and content adaptation take place in a “trusted zone”
- Adaptation TVM is therefore self-contained
  - contains Decryption module
  - contains CP-TVM
- License may limit adaptation capabilities
- The DID Descriptors that deal with e2e QoS never get encrypted



Thank You !