Secure Renewability of Compromised IPMP Tools

Beilu Shao
EPFL
WIAMIS' 08, May 07 2008
Klagenfurt, Austria

Outline of the Presentation

- Problem Statement
- Challenges and Opportunities
- Proposed Solution
- Conclusions
- Acknowledgement
- Q&A

The Big Picture

- Problems with Digital Rights Management (DRM) systems
  - inter-operability
  - Renewability
- Standards activities
  - MPEG-4 IPMP
  - MPEG-4 IPMP-X
  - MPEG-21 IPMP
  - DMP

DRM Renewability Problem

- What is "*Renewability*"?

  to make like new, restore to freshness, vigor, or perfection

  --- *Merriam-Webster Dictionary*

  renewable substances can be used and easily replaced, e.g. renewable energy resources

  --- *Cambridge Dictionary*

  DRM: robustness and flexibility, where one can easily renew a broken DRM system

- Why this problem?

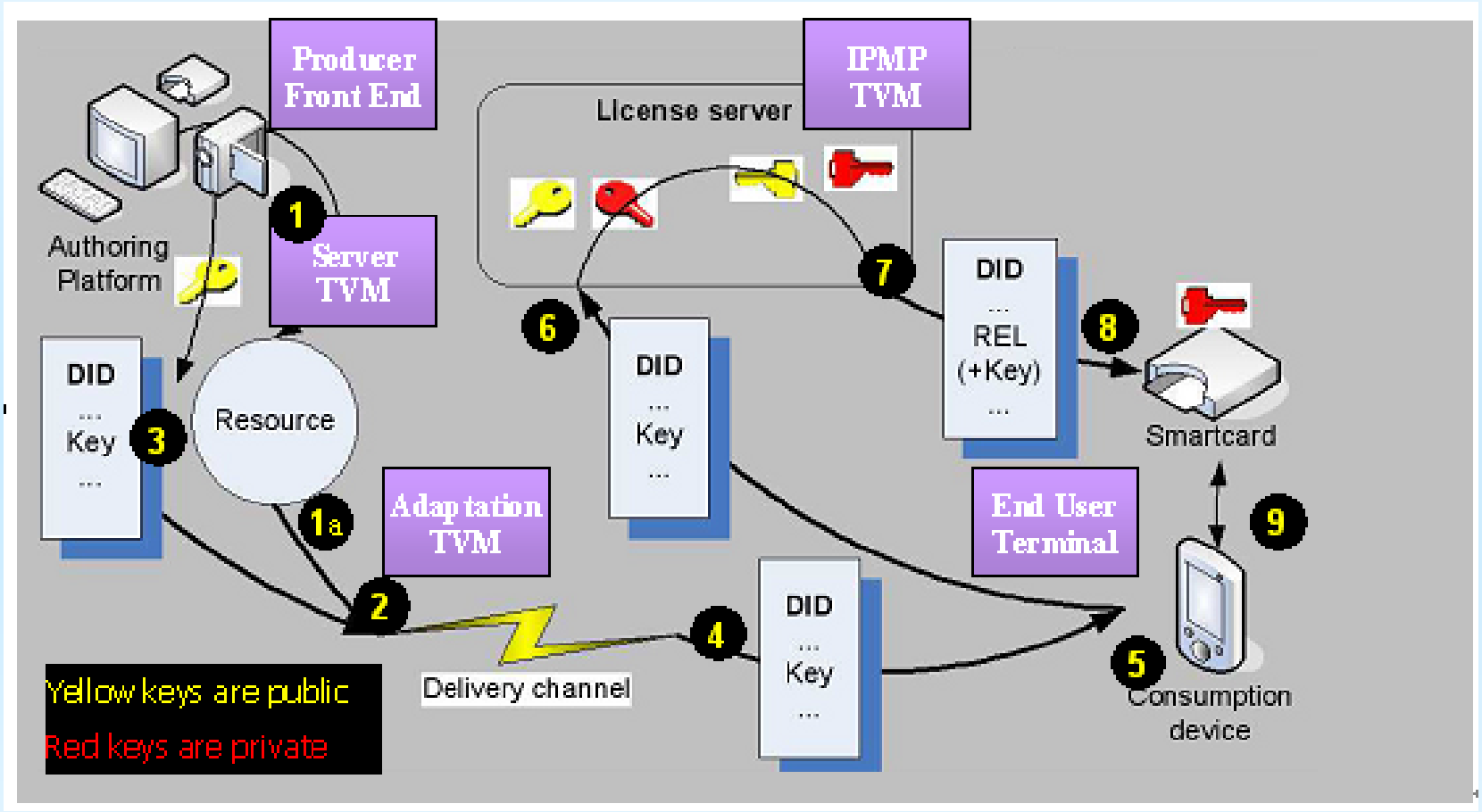
  DRM systems are subject to possible attacks. Without renewability, the DRM system has little means for recovering after security has been compromised

ENTHRONE E2E DRM Design

Challenges and Approaches

- DRM inter-operability problem: MPEG-21 DID/REL
- Super-distribution problem: Sharing License/Domain License
- Usage rights protection enforcement problem: smartcard
- Domain management problem: key sharing

ENTHRONE DRM Framework Overview



Overview of MPEG IPMP Renewability

- IPMP Tool List:

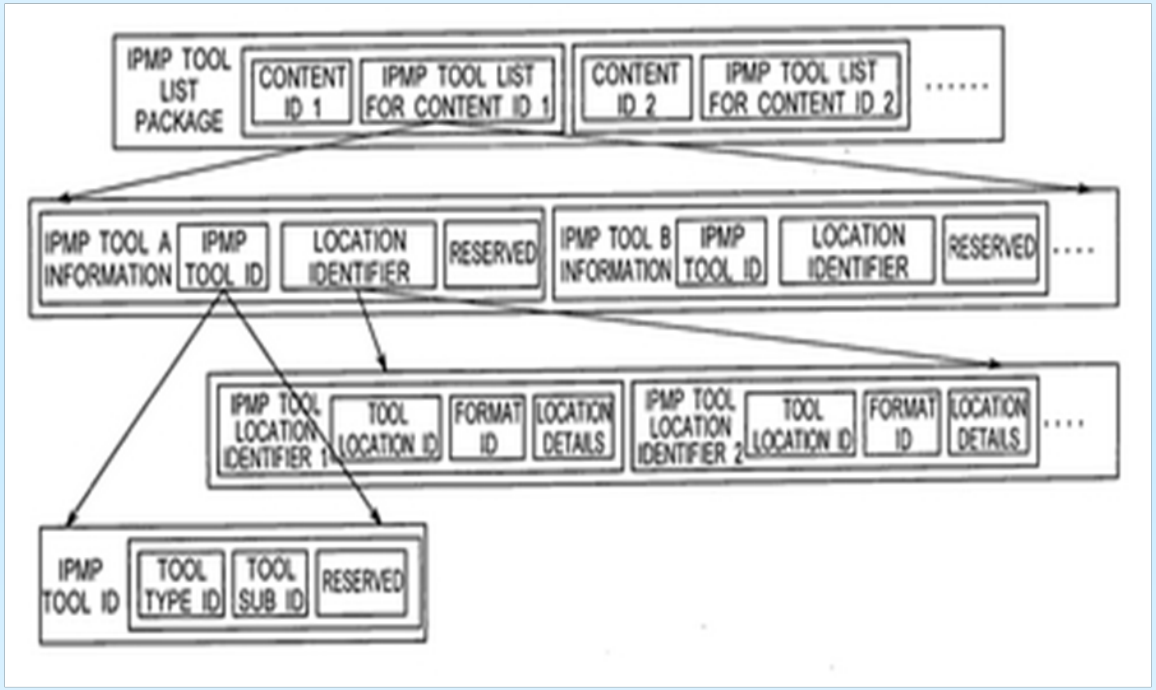
  enlist the information of the tools required by the terminal to decode the protected content. This mechanism enables the terminal to select or renew the tools, or to retrieve the tools when they are missing

- IPMP Tools:

  modules performing (one or more) IPMP functions such as authentication, decryption, watermarking, etc. Each IPMP Tool has a unique IPMP Tool ID.

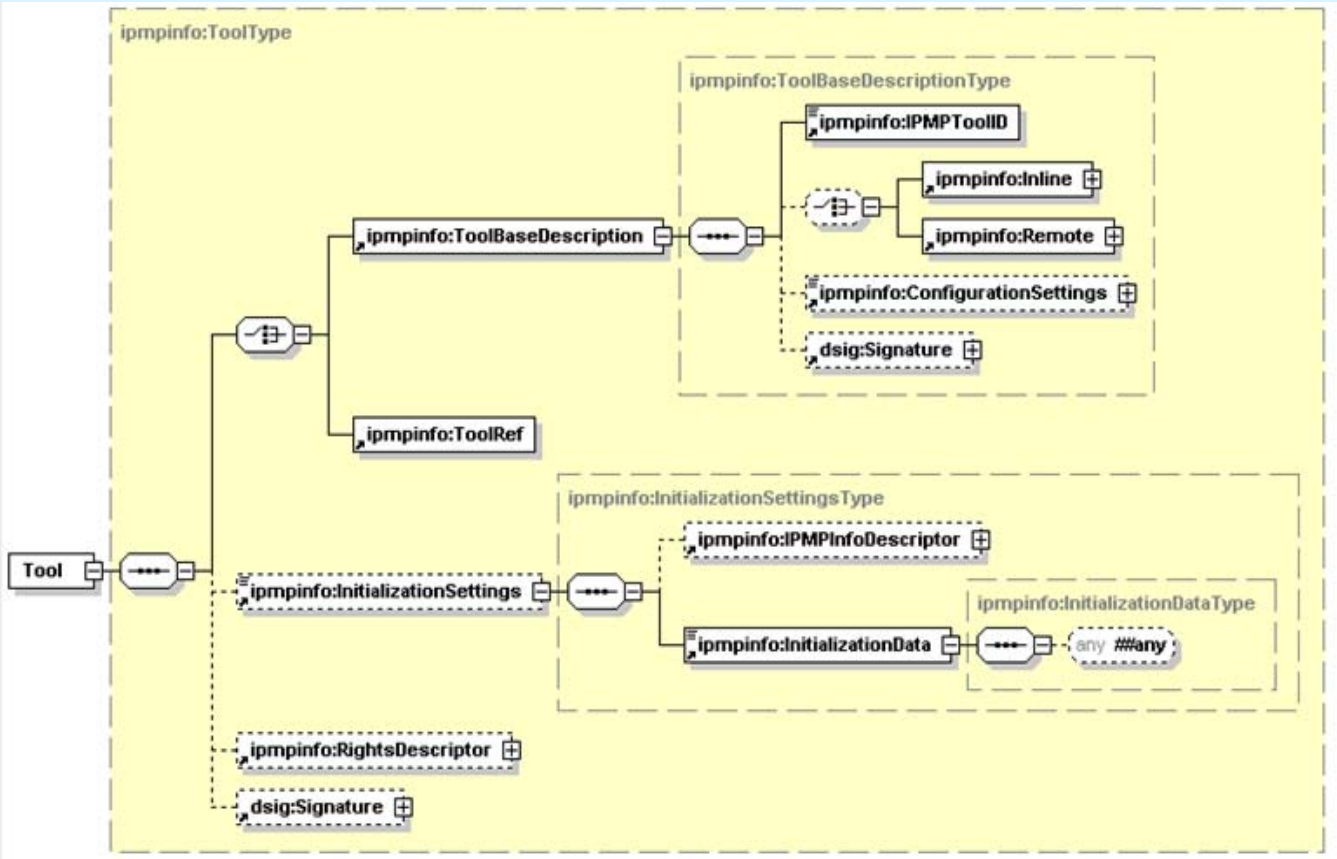
Overview of MPEG IPMP Renewability

- MPEG-4 IPMP-X



Overview of MPEG IPMP Renewability

- MPEG-21 IPMP



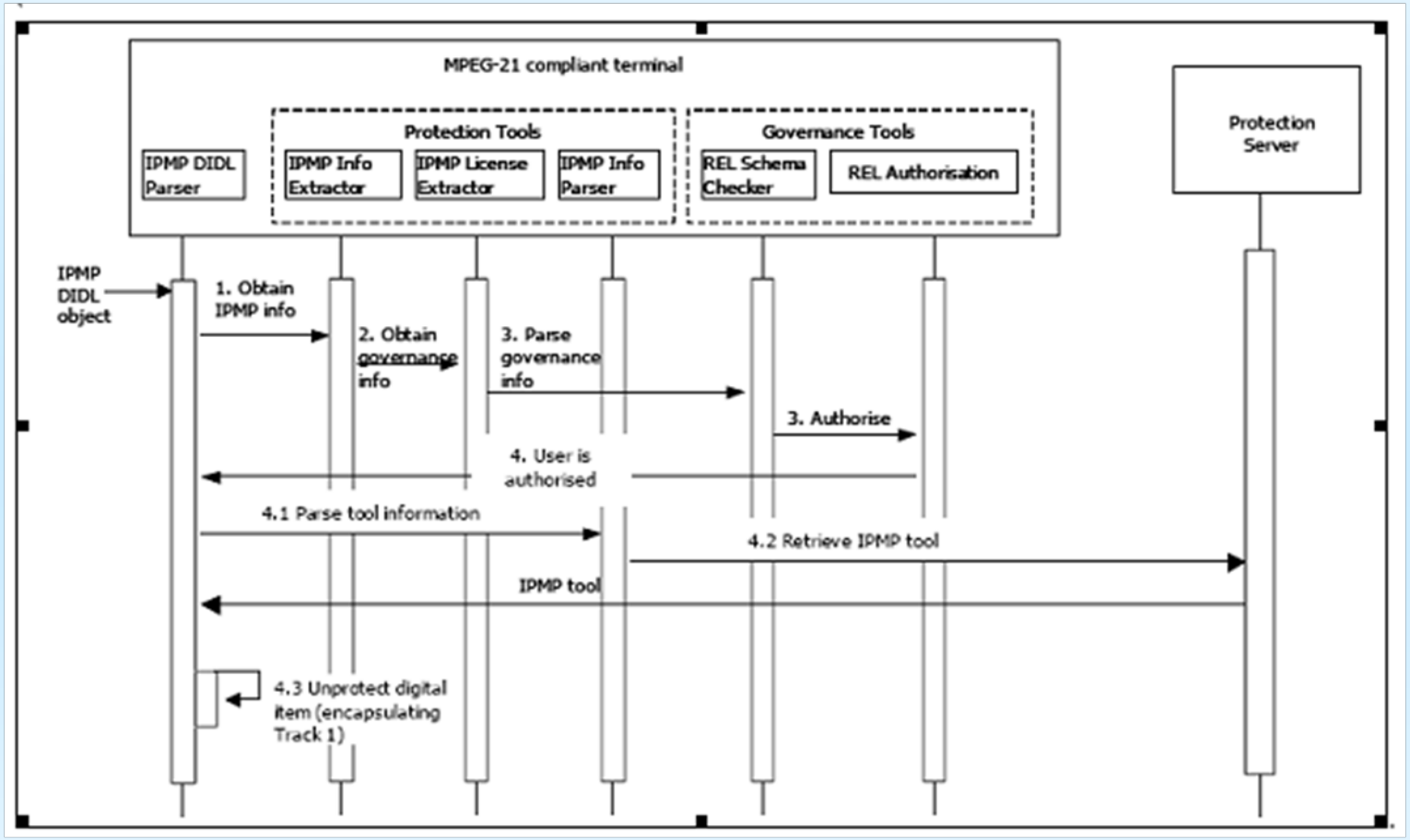
IPMP Renewability Solutions in ENTHRONE

- Redefined Schema
  1. IPMP DIDL;
  2. IPMP Info;
  3. IPMP General Info
- Integration with the ENTHRONE E2E Protection System
  1. Authoring side
  2. Consumption side

Renewability Solutions in ENTHRONE

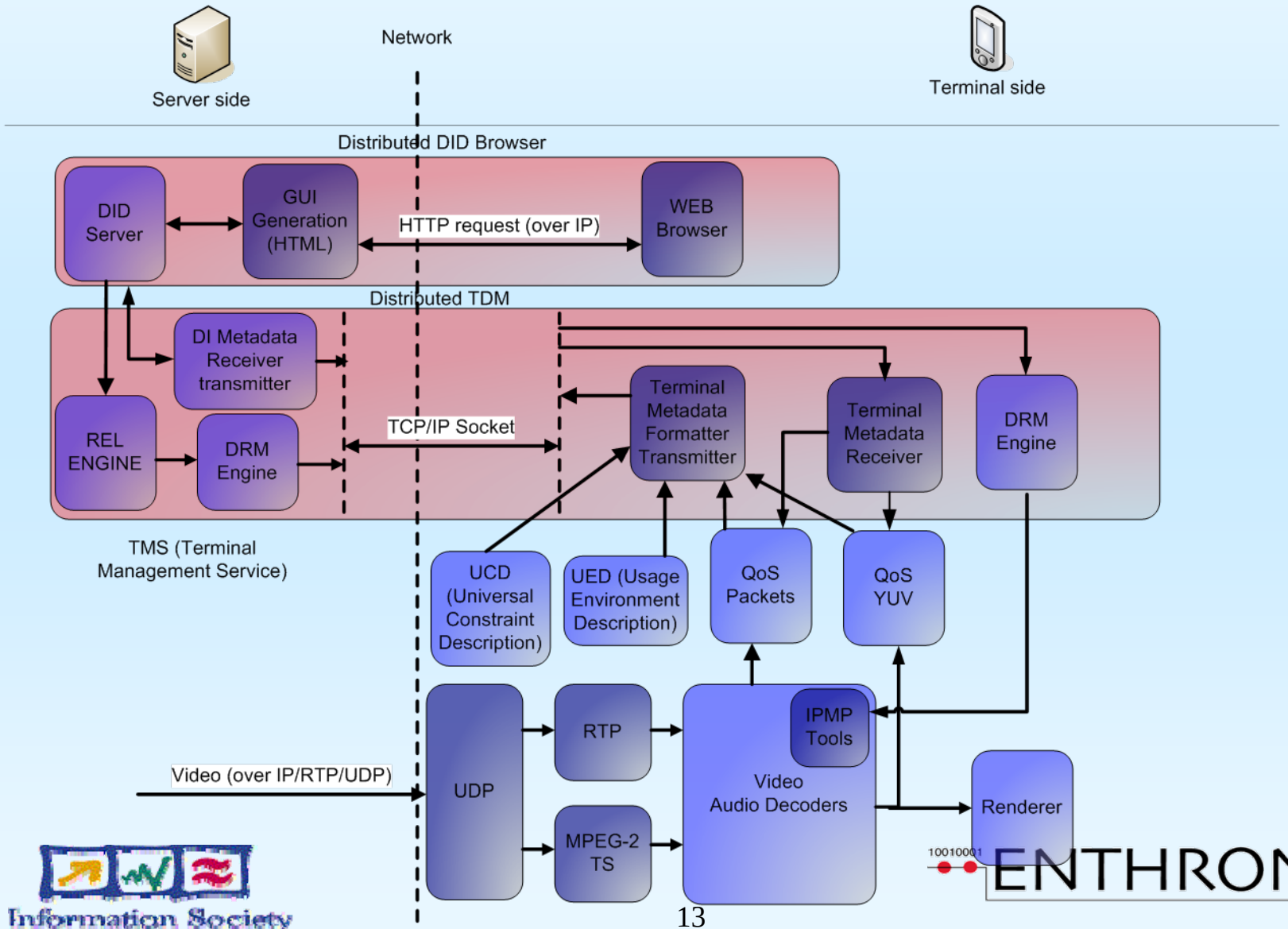
1. The input IPMP information is parsed in order to get the IPMP Tool List. If there is no list, operation skips to step 4, otherwise the IPMP Tool Information in the IPMP Tool List is parsed.
2. If the AES Decryptor Tool is available on the Terminal and it has not been compromised, operation skips to step 4.
3. The IPMP Tool Manager looks for the required IPMP Tool: if the search is successful, operation stops; otherwise, operation advances to step 4.
4. After the acquisition of the IPMP Tool, the protected content can start flowing into the data buffer.

Walkthrough of the Rights Acquisition

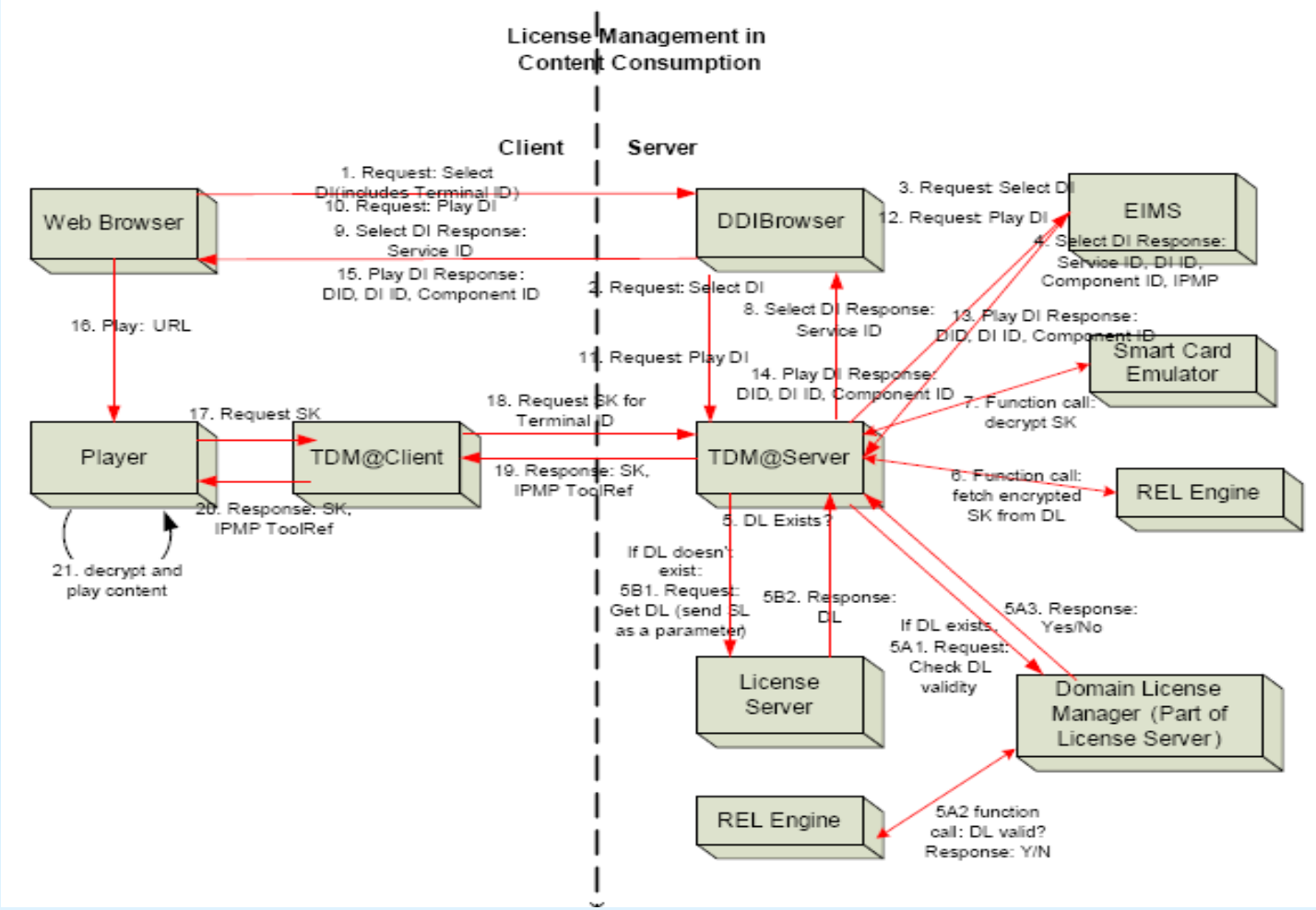


WP-7: ENTHRONE 2 Achievements

ENTHRONE 2 Terminal Architecture



Integration and Application Scenario



Conclusions

- Renewability solutions through MPEG-21 IPMP
- Successfully integrated with EHTHRONE E2E DRM
- Another prototype application for MPEG-21

Acknowledgement

- ENTHRONE II Project: EU Framework Program 6 for Research and Development
- ENTHRONE II Partners, in particular:

  Itsik Arbel, Adi Alter, Alex Chernilov (Optibase)

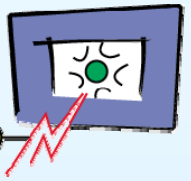
  Daniele Renzi, Stefano Battista (bSoft)

  Helder Castro, Giorgiana Ciobanu (INESC, Porto)

  Artur Lugmayr (TUT)

  Ingo Kofler, Michael Ransburg (UNIKLU)

  Samuel Keller, Marco Mattavelli (EPFL)



Thank you for your attention!

Questions?