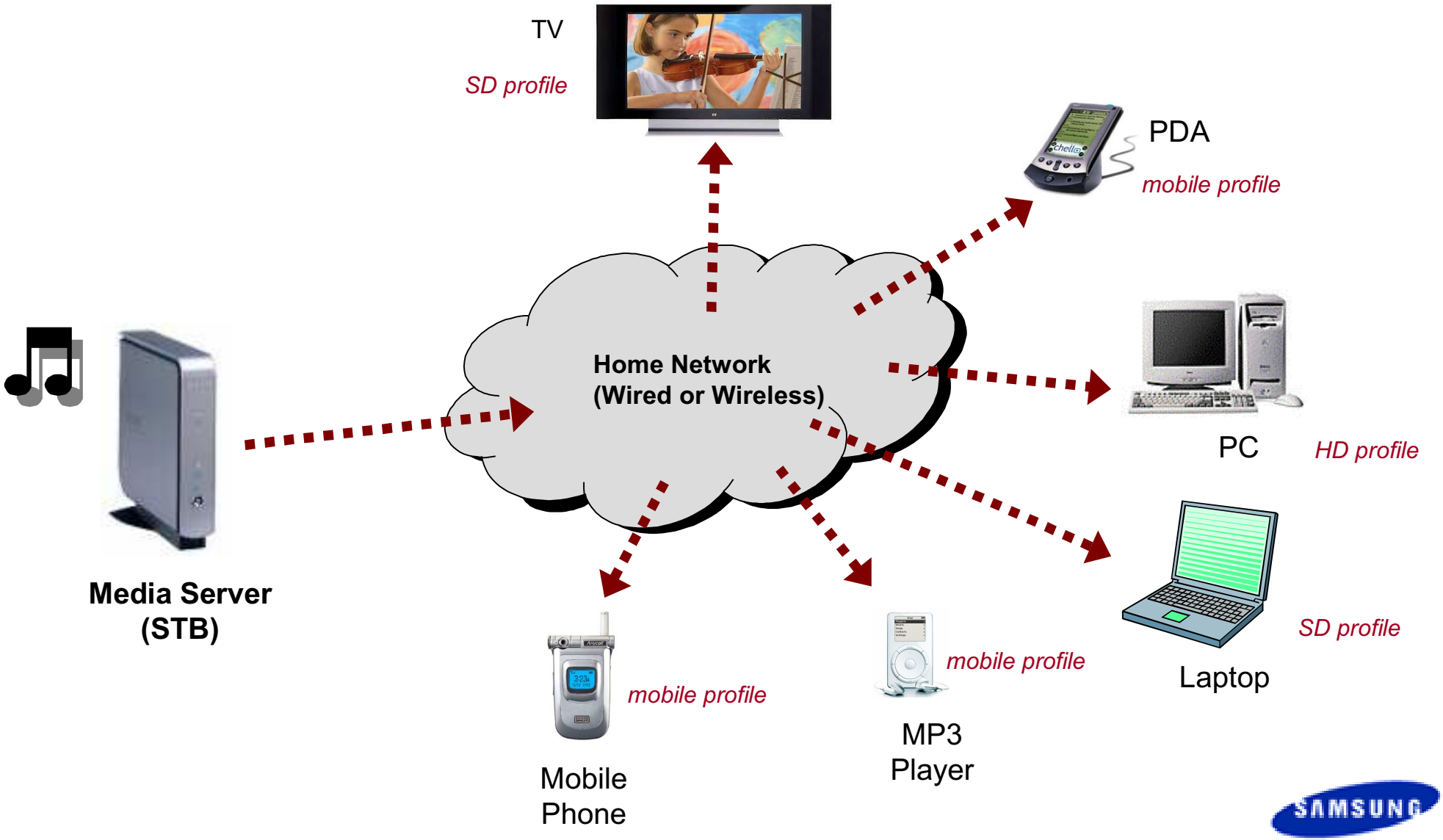
Scalable DRM System for Media Portability

Hyoungshick Kim

Samsung Electronics

SAMSUNG

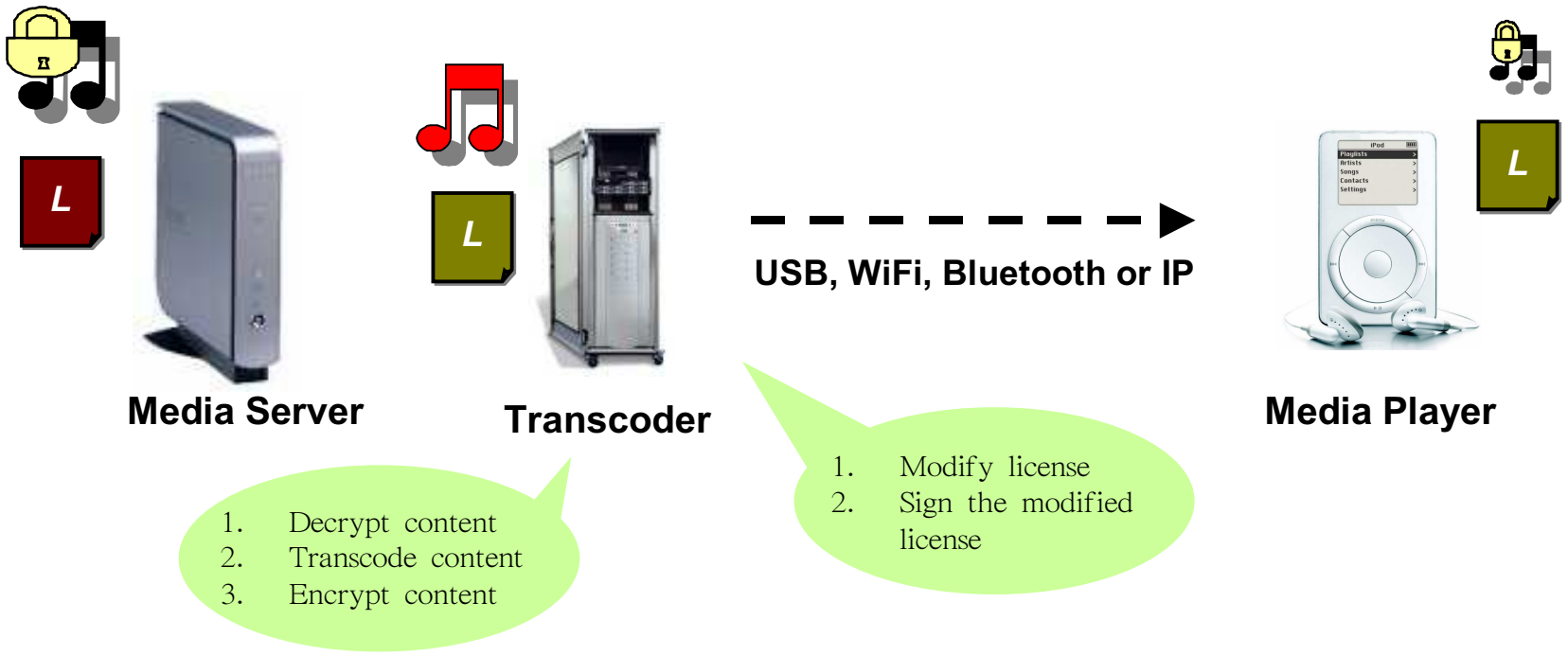
There are several playback devices with different device capabilities.



Media Portability for protected contents

Transfer media content from a source device to a sink device.

- Example: A consumer wants to transfer content from his STB to his portable player.



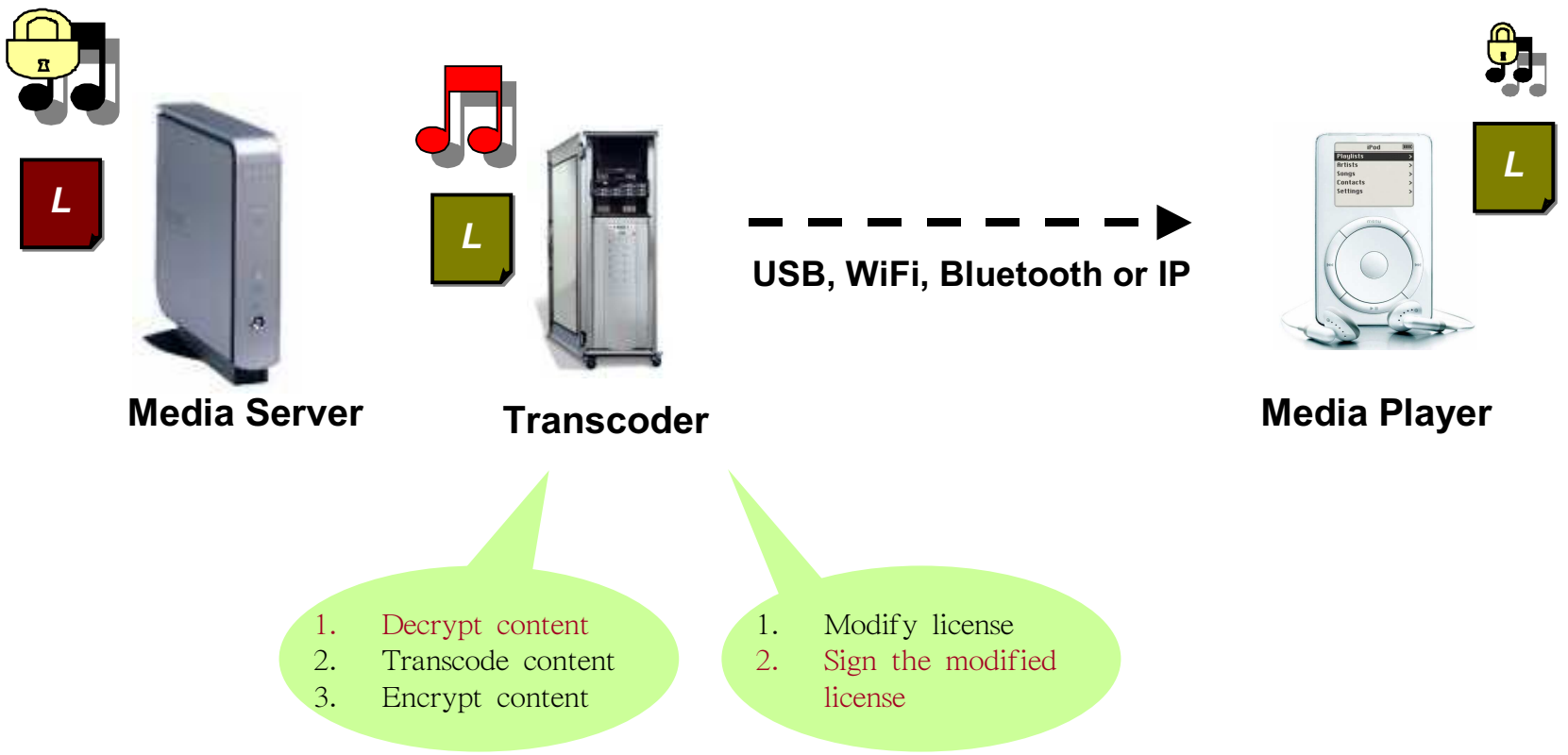
- End-to-end security should be maintained.
- Cost of moving contents should be minimized.
- Scalability should be provided for heterogeneous environment.
- Changes to existing DRM solutions should be minimized

SAMSUNG

Related Work

- Localized (trusted) transcoder
  - Local generation of license using proxy signature [KLCYLK06]
  - Domain/Rights intermediate manager [TCG06][KM05]
- DRM interoperability using peer-to-peer network connections [BM04][SSU04][KLMM04]
  - Coral, OPERA standardization
- DRM interoperability based on Full-format [SSU04][KLMM04]
  - OMA DRM standardization
- Configuration-driven DRM interoperability [SUKSNJZS04]
  - Standardizing DRM interoperability using hooks placed in the content's metadata
- Interoperability for Rights expression language [SSU04][CM05]

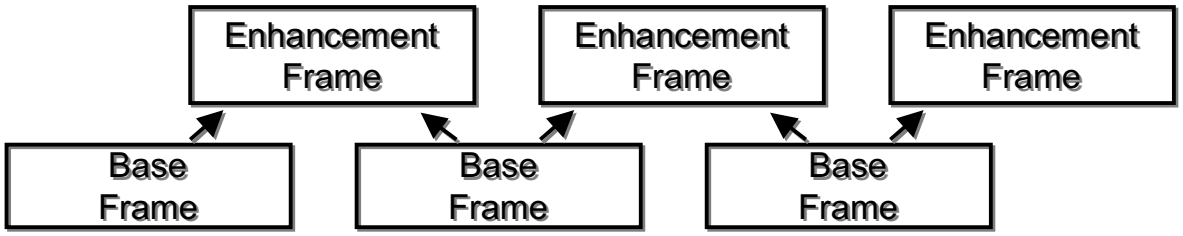
Revisited Problems



- How can we transcode contents without decryption/re-encryption?
- How can we sign the license without the contents owner's sign key?
- How can we design the proposed system which is compatible with the existing DRM solutions (e.g. OMA DRM) ?

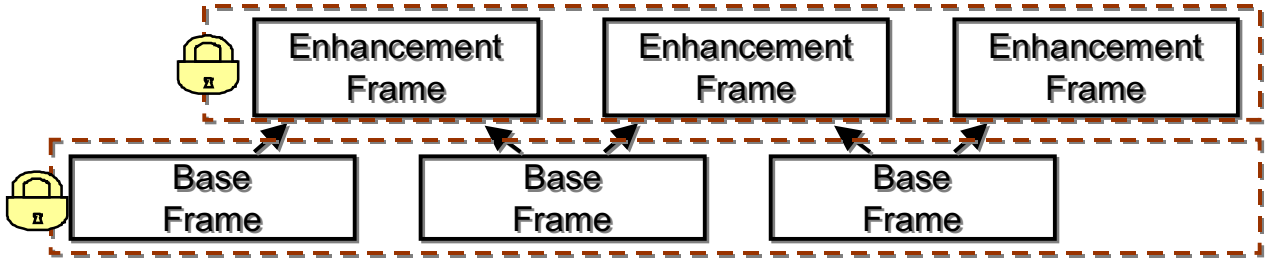
Layered Coding [RSW06]

Base layer coded at lower frame rate
Enhancement layer provides in-between frames at higher frame rate (MPEG4-SVC, JPEG 2000)



Progressive Encryption

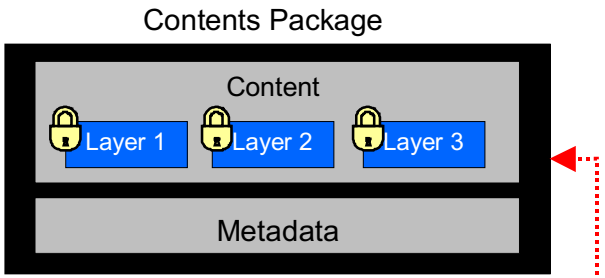
Independent encryption of each layer



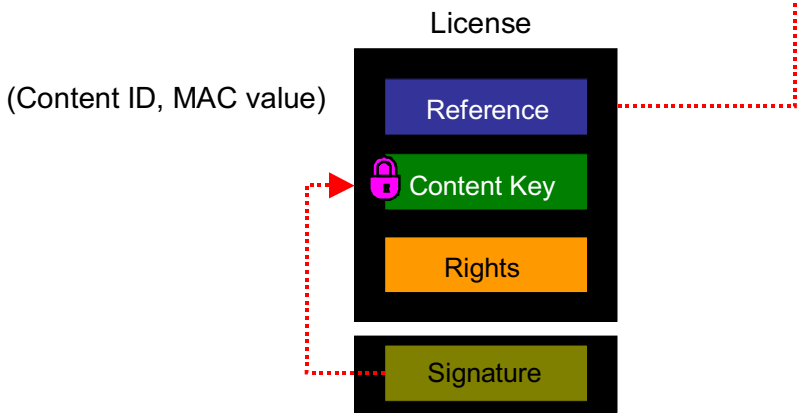
- Partition data into layers
- Data in each layer is encrypted by block cipher algorithm

We design the protected contents package/license compatible with OMA DRM DCF/License using scalable coding and progressive encryption.

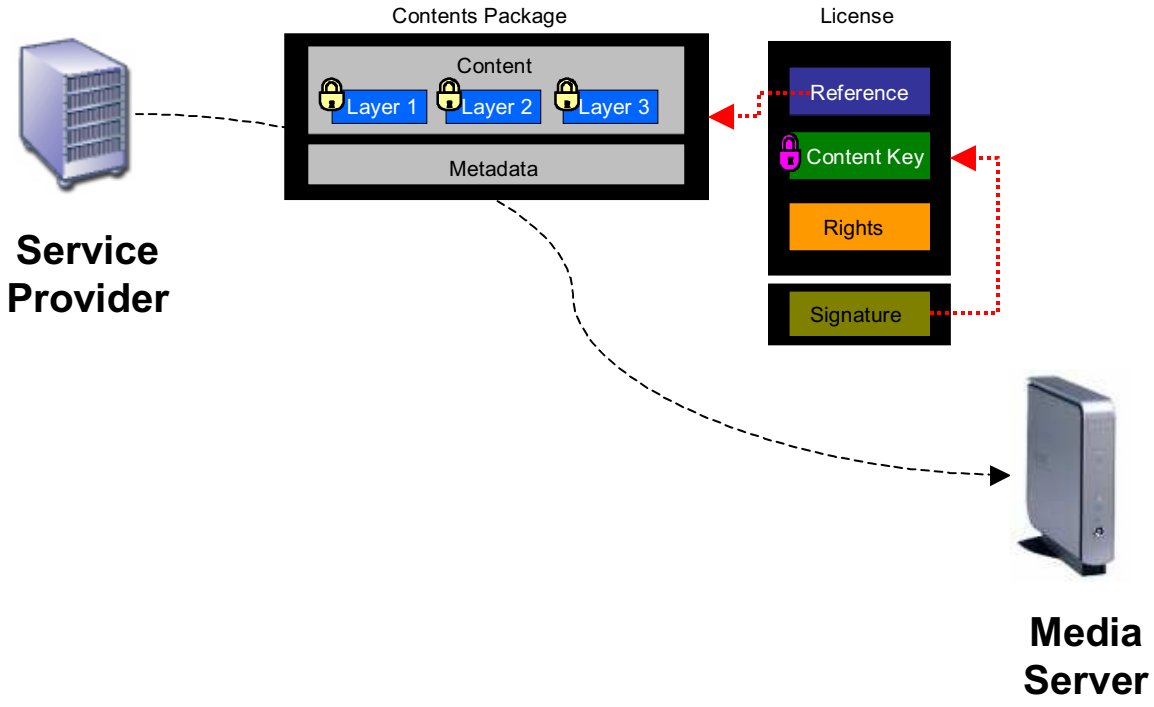
Contents Package



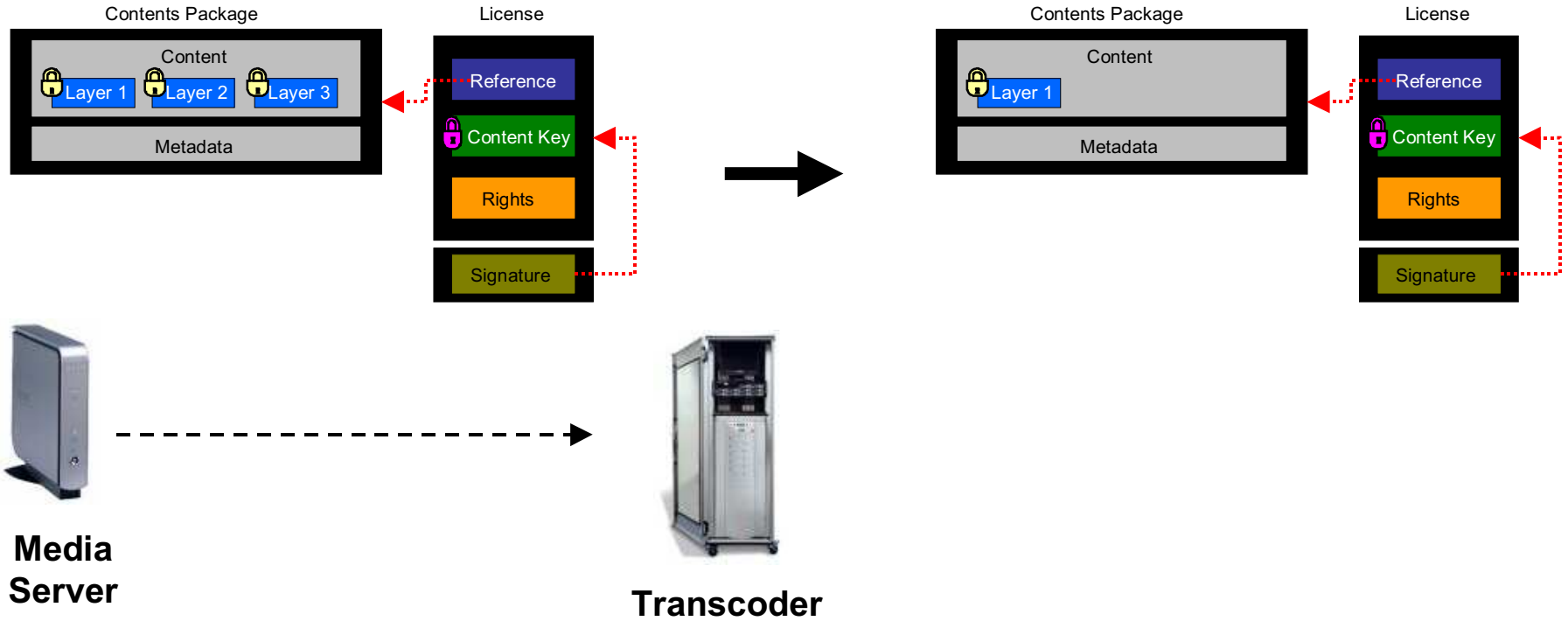
DRM License



After purchasing contents, Media Server downloads the contents package and license.



Transcoder translate the protected contents for a specific AV profile.

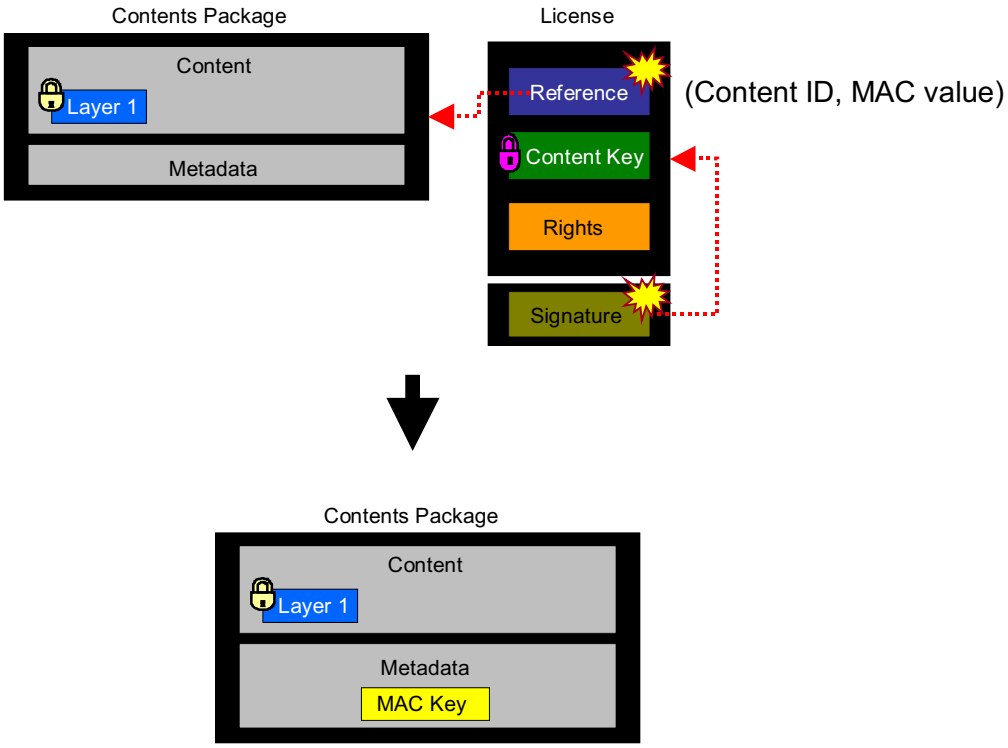


The transcoder simply truncates needless layers. It is not required that the specific compression, decoding, or encryption algorithms are implemented in the transcoder.

Update of MAC

Leading the Next

How can the Transcoder compute the updated MAC value and the signed value without the signing key?



We add the MAC Key to the Metadata.

The integrity of the MAC Key is guaranteed by the signature.

Signature of DRM License

Leading the Next

Notation

D : a group with operation *

Hash Function $H:\{0,1\}^* \rightarrow D$

π : $D \rightarrow D$, trapdoor permutation with a trapdoor t

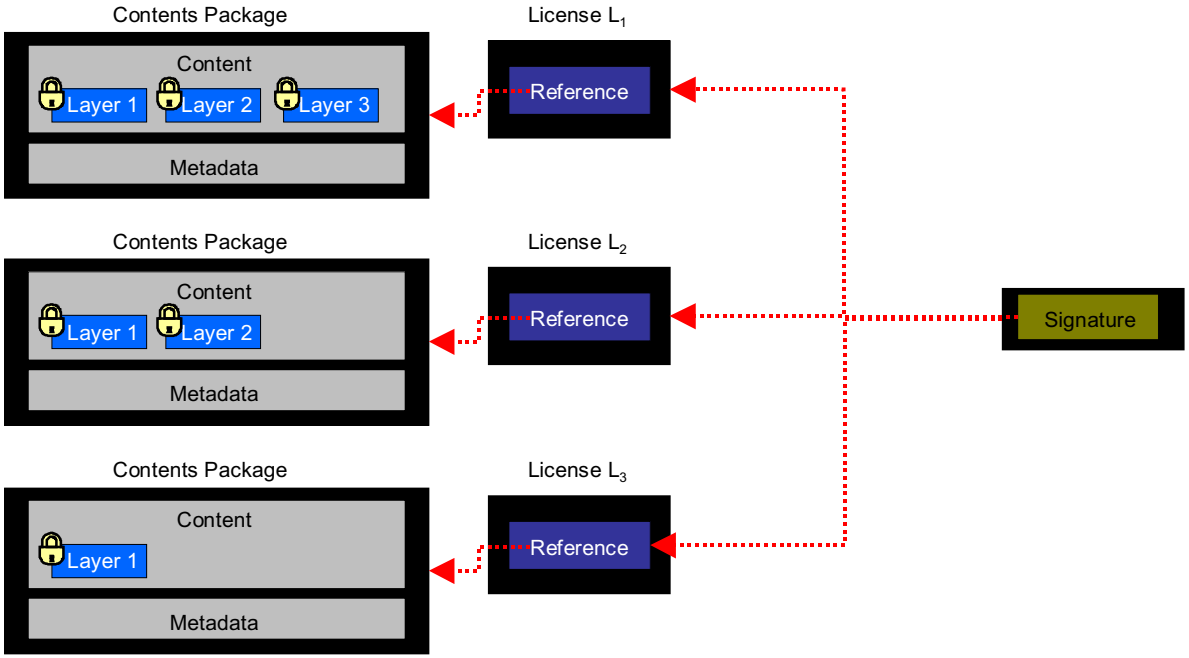
Key Generation

Service Provider's Signing key : trapdoor t

Service Provider's Verification key : trapdoor permutation π

Signing

Signature $\sigma_1 = \pi^{-1}(H(L_1) * \pi^{-1}(H(L_2) * \pi^{-1}(H(L_3))))$



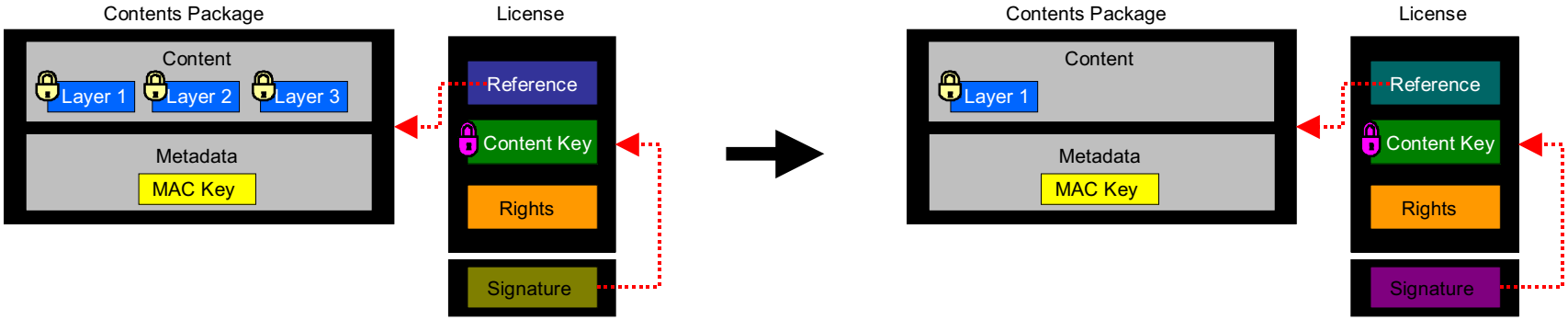
SAMSUNG

Update of Signed Values

Leading the Next

Transcoder simply compute the updated signed value using the public Service Provider's verification key π .

$$\text{Signature } \sigma_3 = \pi^{-1}(H(L_1) * \pi^{-1}(H(L_2) * \pi^{-1}(H(L_3))))$$



Player can check whether the following computed result is a unit of the group D.

$$H(L_3)^{-1} * \pi(\sigma_3)$$

SAMSUNG

- Propose new DRM model for media portability.
  - ✓ No secure transcoder
  - ✓ Simple/Efficient transcoding
  - ✓ Compatible with existing solutions

Questions?

References

[KLCYCK06] H. Kim, Y. Lee, B. Chung, H. Yoon, J. Lee, K. Jung.: Digital Rights Management with Right Delegation for Home Networks, Information security and cryptology ICISC 2006, pp. 233--245 (2006).

[TCG06] Gelareh Taban, Alvaro A. Cardenas, Virgil D. Gligor.: Towards a secure and interoperable DRM architecture, In: Proceedings of the 6th ACM Workshop on Digital Rights Management, pp.69--78 (2006).

[KM05] David W. Kravitz, and Thomas S. Messerges.: Achieving media portability through local content translation and end-to-end rights management, In: Proceedings of the Fifth ACM Workshop on Digital Rights Management (2005).

[BM04] W.B. Bradley and D.P. Maher.: The NEMO P2P service orchestration framework, In: Proceedings of the 37th Hawaii International Conference on System Sciences (2004).

[SSU04] R. Safavi-Niani, N. Sheppard, and T. Uehara.: Import/Export in digital rights management, In: Proceedings of the 4th ACM Workshop on Digital Rights Management, pp. 99--110 (2004).

[KLMM04] R.H.Koenen, J.Lacy, M.Mackey, and S.Mitchell.: The long march to interoperable digital rights management, In: Proceedings of the IEEE, vol. 92(6) (2004).

[SUKSNJZS04] T. Senoh, T. Ueno, T. Kogure, Shen Shengmei, Ji Nfing, Liu Jing, Huang Zhongyang, C.A. Schultz.: DRM Renewability & Interoperability, Consumer Communications and Networking Conference, Jan 2004 (2004).

[CM05] Brenton Cooper, Paul Montague.: Translation of Rights Expressions, ACSW Frontiers 2005, pp. 137--144 (2005).

[RSW06] J. Reichel, H. Schwarz.: M. Wien, Joint Scalable Video Model JSVM-6, Doc. JVT-S202 (2006).