# Information Security

## Supplementary

Eom, Hyeonsang (엄현상)
Department of Computer Science & Engineering
Seoul National University (SNU)

2022.5.17
서울대학교 우리은행 교육과정 핀테크 산업 응용 2차시 강의 파트 II

# Outline

- Supplementary
  - Example: Information Protection
  - Review: PKI Example
  - More about DRM Example
- Q&A

# Example: Information Protection

- ATM PIN Security
  - Splitting of a Customer's PIN into Two Parts and Storing Them Separately
    - PIN Offset in the ATM server
    - Natural PIN derived with the PIN key in the PIN machine

CustomerPIN =(?) f(Acct#, PINOffset, PINKey)

Natural PIN Is Not Stored Anywhere in the Entire Process

# Review: PKI Example

- Basics
  - Digital Signature (DS)
    - DS(I,pr) for Information I and a private key pr
  - Certificate C (Containing a Public Key and DS)
    - C(pu,prO) for a public key pu and prO from CA


Used to Make DS in C (by Encrypting the Rest of C)

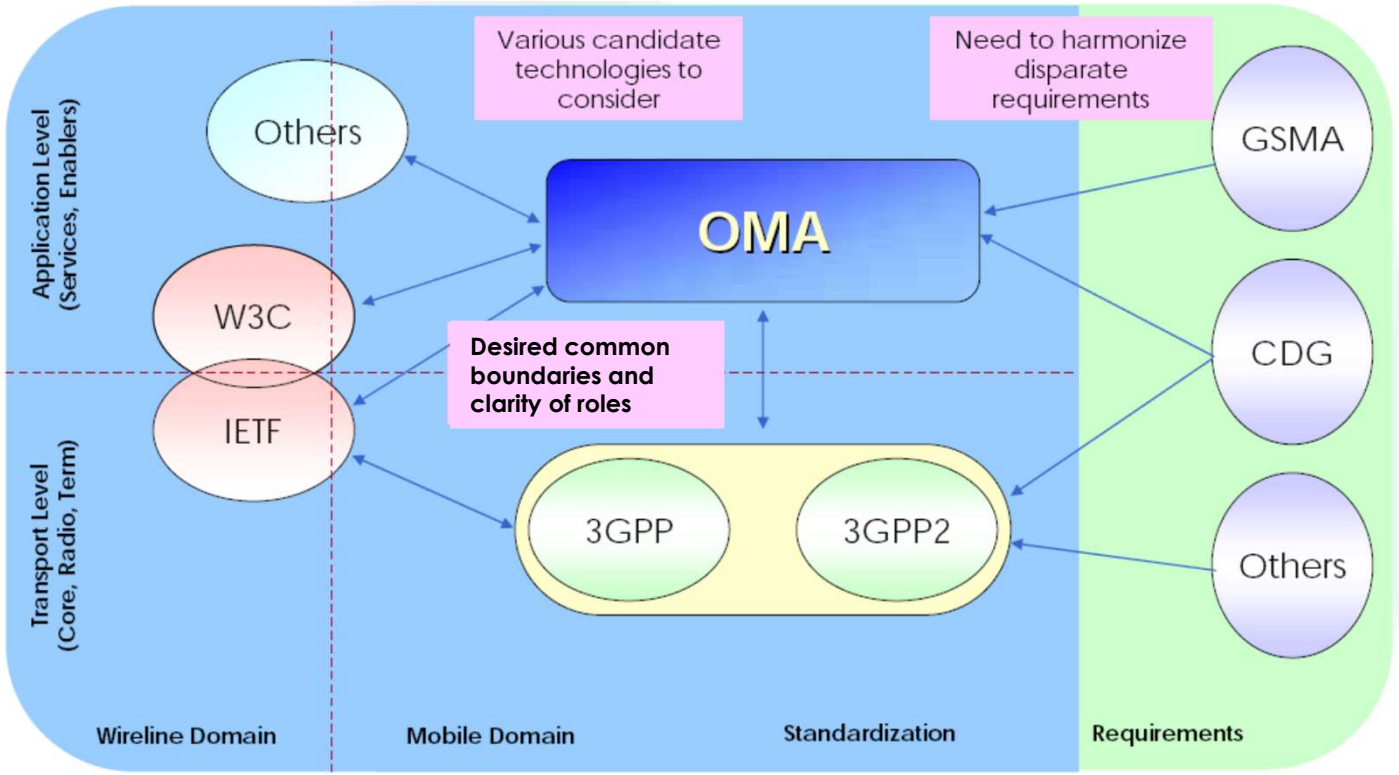
- Question
  - Is This Secure?
    - A sends B I+DS(I,pr1)+C1(pu1,prO)
    - B verifies C1(pu1,prO) by obtaining CO(puO,prO) from CA
      - Verification with DS of C1(pu1,prO), and puO
    - B verifies DS(I,pr1) with pu1

Self-Signed

# More about DRM Example

- DRM Example: OMA (Open Mobile Alliance) DRM
  - Open Mobile Alliance
  - Overview of OMA DRM V1.0
  - Overview of OMA DRM V2.0
  - DRM Architecture
  - Domains
- Summary

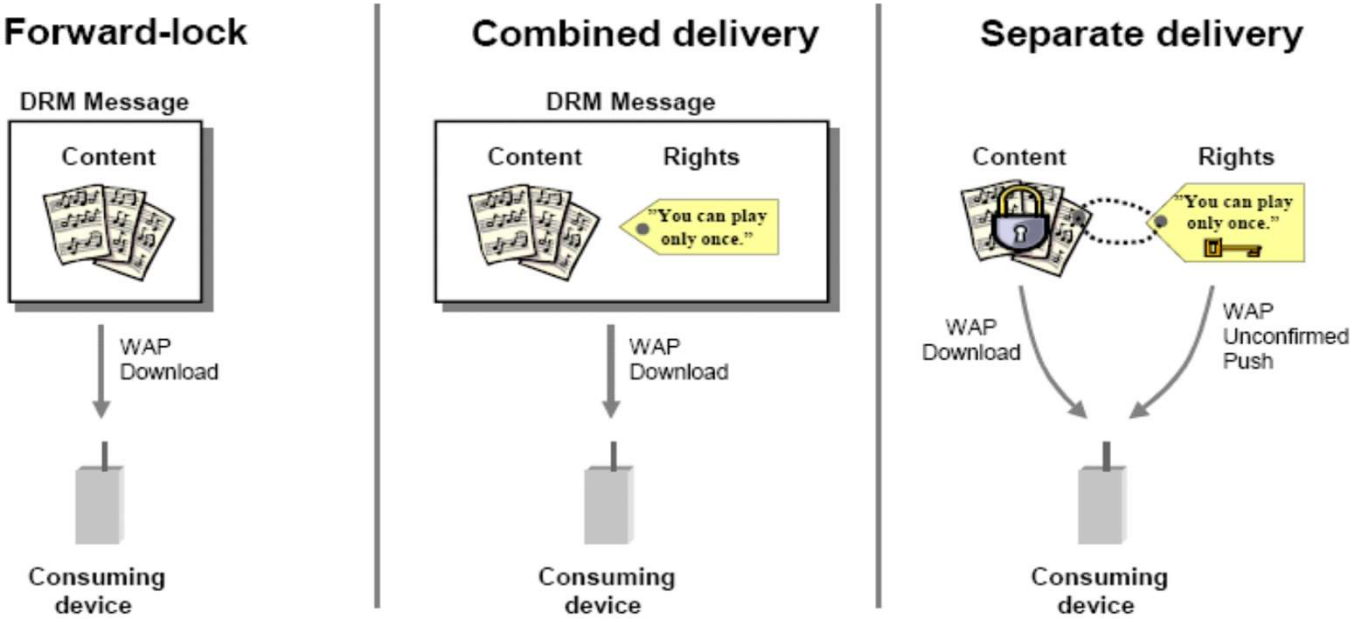
# Open Mobile Alliance




GSMA : Global System for Mobile communication Association
CDG : CDMA Development Group
3GPP : 3rd Generation Partnership Project
W3C : World Wide Web Consortium
IETF : Internet Engineering Task Force

# Overview of OMA DRM V1.0

- To

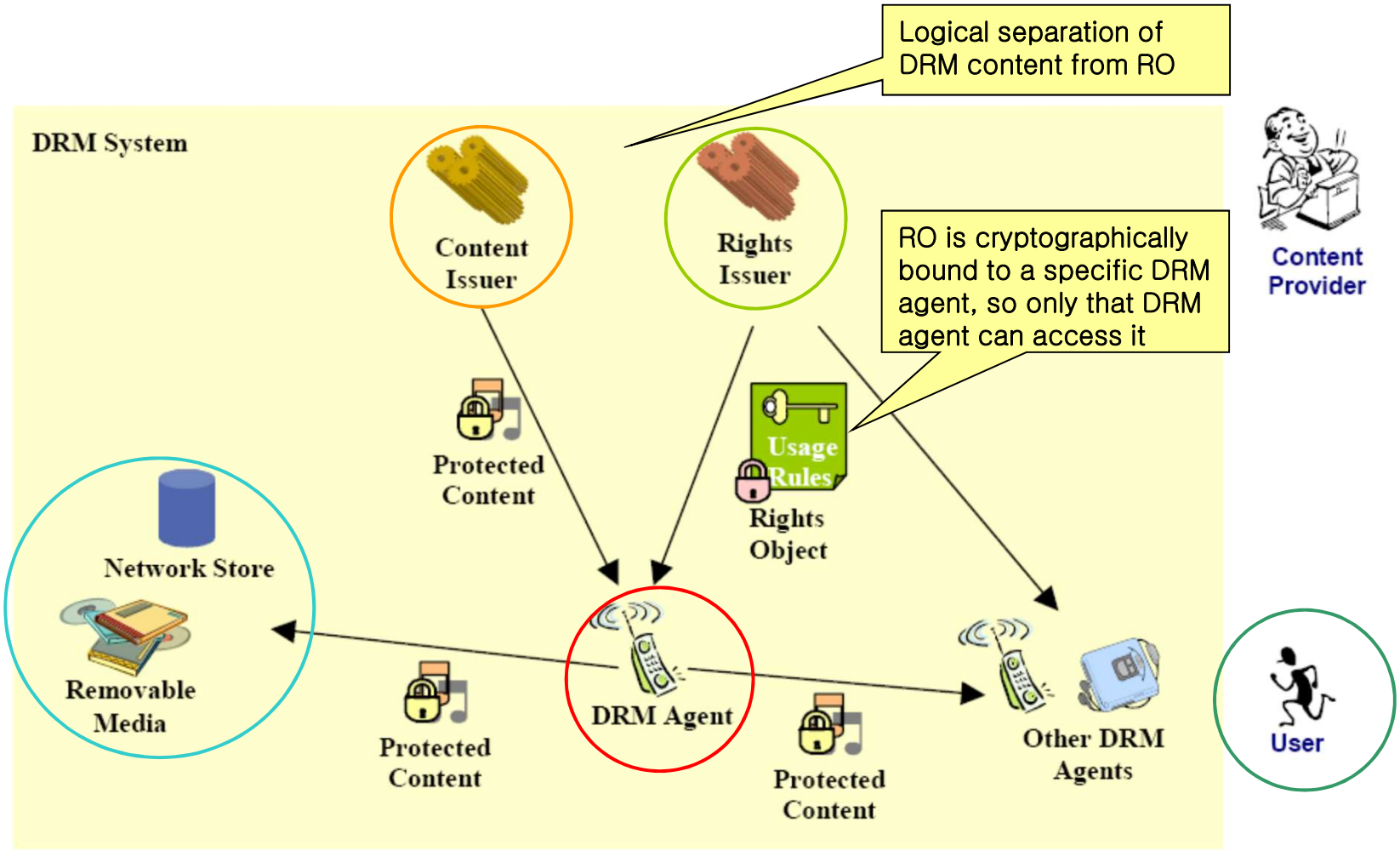



| | | |
|---|---|---|
| • Prevent peer-to-peer distribution of low-value content<br>• Prohibit device from forwarding content to other devices<br>• Consider only one media object | • Define a rights object containing permissions and constraints<br>• Package both content and a rights object in a DRM message | • Protect higher value content using encryption<br>• Separate content and a rights object<br>– Protected content delivered over any medium<br>– Rights object delivered via WAP push |

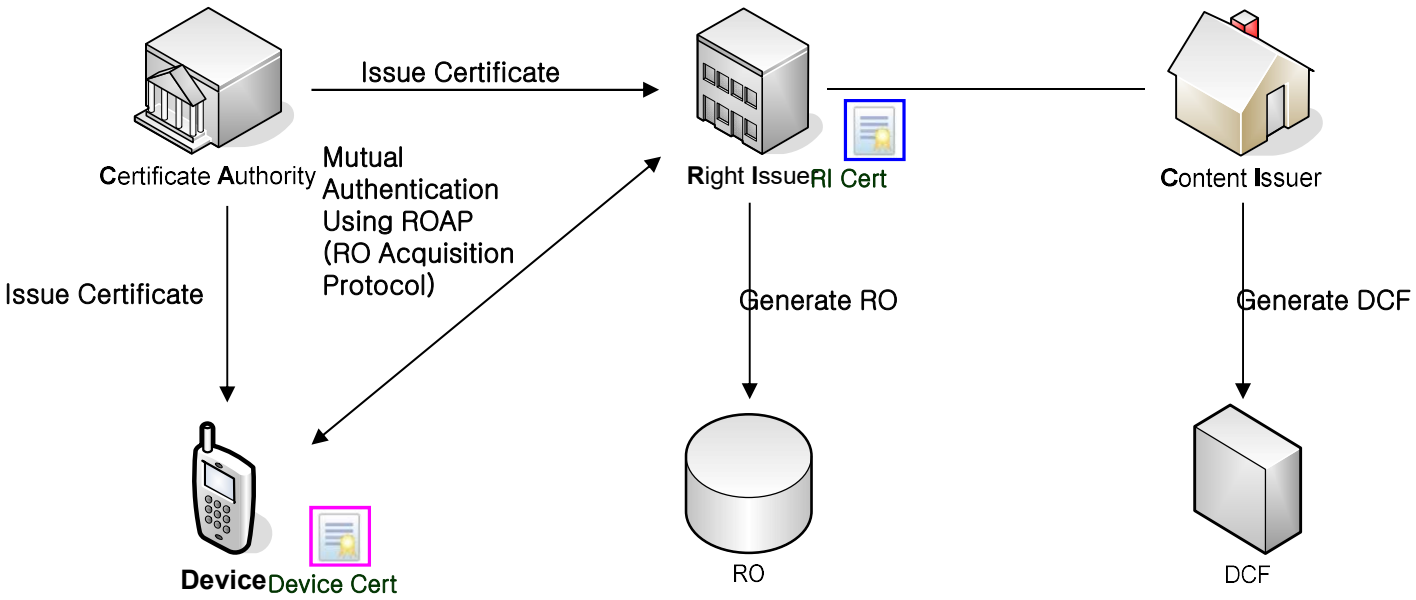
# Overview of OMA DRM V2.0

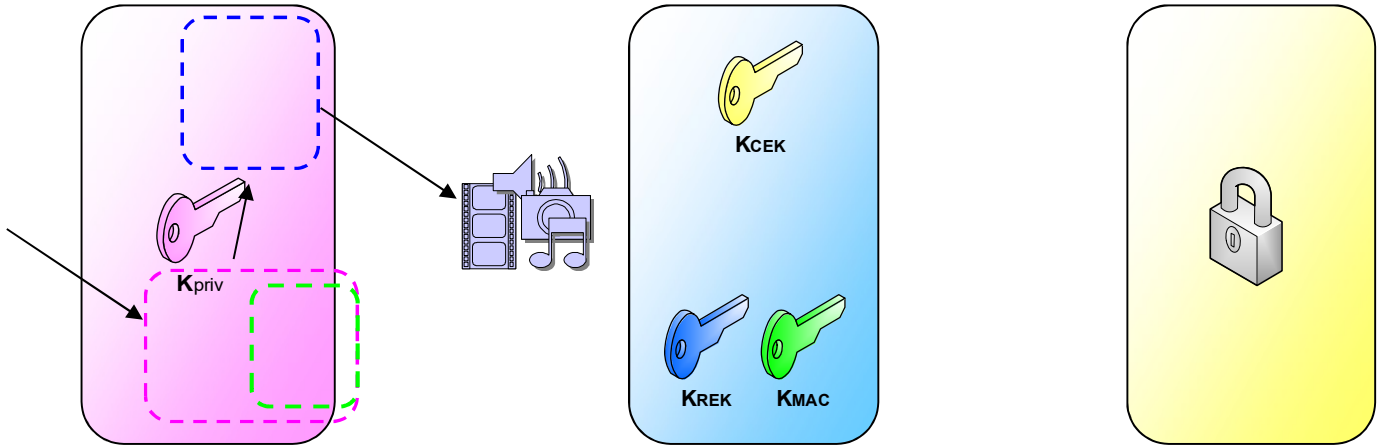
- Target
  - Enhanced Protection of Premium Content
    - Basic Pull Model
    - Push of DRM Content
    - Streaming of DRM Content *(Added)*
    - Domains *(Added)*
    - Backup *(Added)*
    - Superdistribution *(Added)*
    - Export *(Added)*
    - Unconnected Device Support *(Added)*

# DRM Architecture



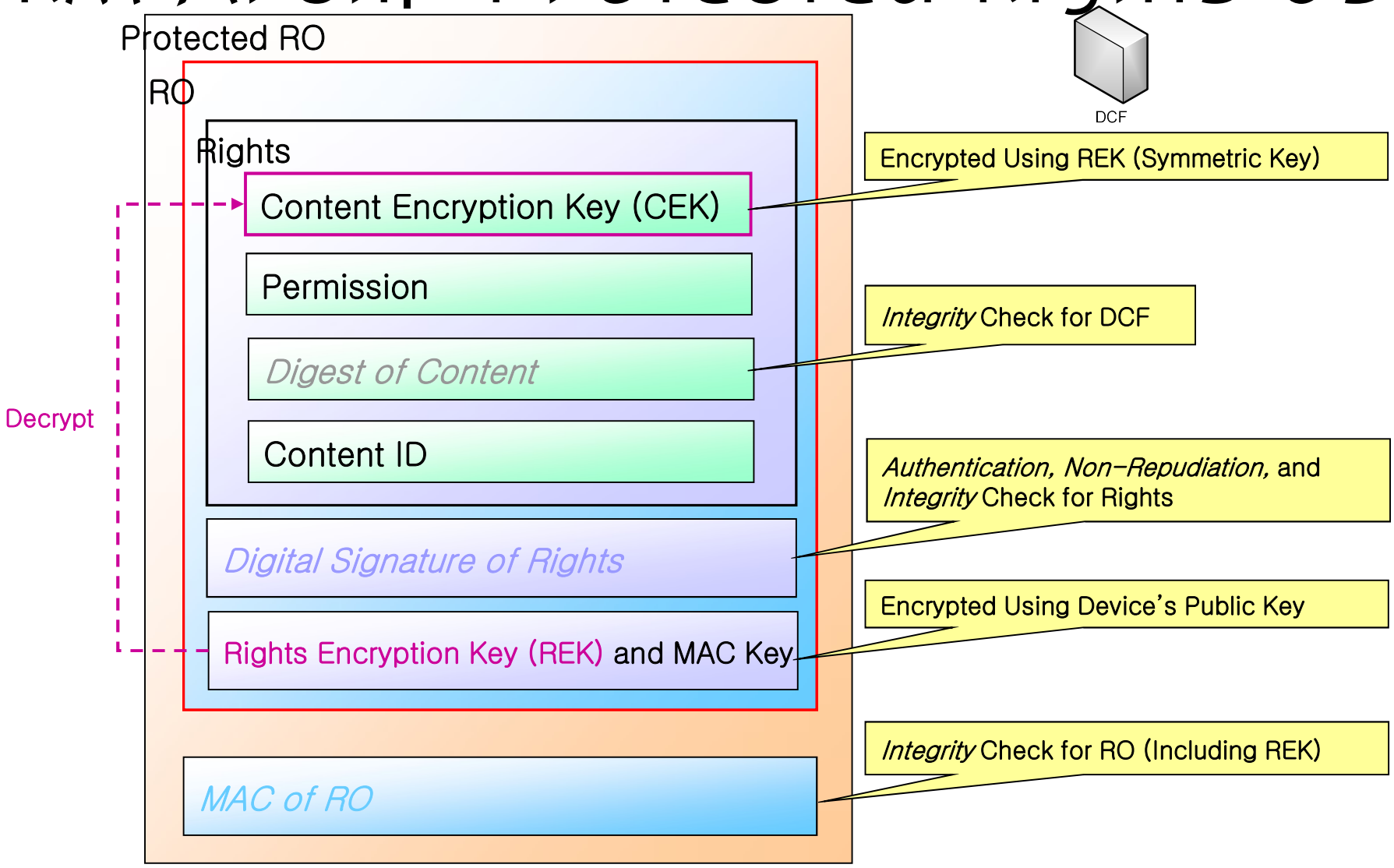
# DRM Arch.: Cryptographic Chain



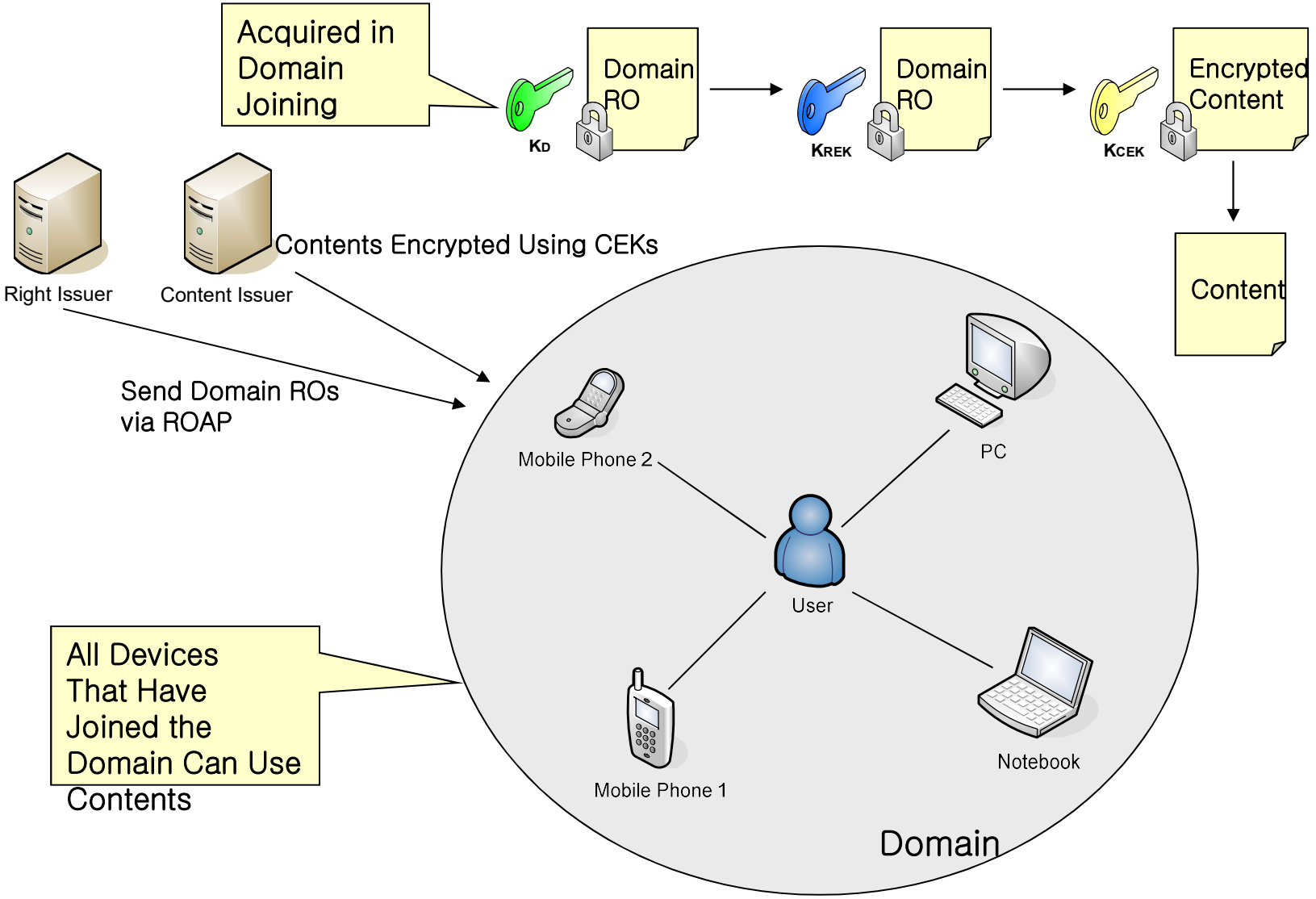




REK Confirmation

# DRM Arch.: Protected Rights Obj.



# Domains



# Thank You!

**Eom, Hyeonsang (엄현상)**

hseom@snu.ac.kr
Department of Computer Science & Engineering
Seoul National University