Outline

- Review
  - Information Protection
  - PKI Example
  - DRM Example

- Q&A
Review: 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,pr0) for a public key pu and pr0 from CA

Question

- Is This Secure?
  - A sends B I + DS(I,pr1) + C1(pu1,pr0)
  - B verifies C1(pu1,pr0) by obtaining C0(pu0,pr0) from CA
  - Verification with DS of C1(pu1,pr0), and pu0
  - B verifies DS(I,pr1) with pu1
Outline: 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

Various candidate technologies to consider
Need to harmonize disparate requirements

Desired common boundaries and clarity of roles

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

MESLab, CSE, SNU
Overview of OMA DRM V1.0

- **Target**
  - Basic Usage of Protected Content
  - Prevent peer-to-peer distribution of low-value content
  - Prohibit device from forwarding content to other devices
  - Consider only one media object

- **Forward-lock**
  - DRM Message
  - Content
  - WAP Download
  - Consuming device

- **Combined delivery**
  - DRM Message
  - Content
  - Rights
  - “You can play only once.”
  - WAP Download
  - Consuming device

- **Separate delivery**
  - DRM Message
  - Content
  - Rights
  - “You can play only once.”
  - WAP Unconfirmed Push
  - Consuming device

- **Prevent higher value content using encryption**
- **Separate content and a rights object**
  - Protected content delivered over any medium
  - Rights object delivered via WAP push

MESLab, CSE, SNU
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

Logical separation of DRM content from RO

RO is cryptographically bound to a specific DRM agent, so only that DRM agent can access it

DRM System

Content Issuer

Rights Issuer

Protected Content

Usage Rules

Rights Object

DRM Agent

Network Store

Removable Media

Protected Content

Protected Content

Other DRM Agents

User

Content Provider
DRM Arch.: Cryptographic Chain

Certificate Authority

Issue Certificate

Mutual Authentication Using ROAP (RO Acquisition Protocol)

Right Issue RI Cert

Generate RO

Content Issuer

Generate DCF

Device

Device Cert

RO

K_{priv}

REK Confirmation

K_{MEK}, K_{MAD}

MESLab, CSE, SNU
DRM Arch.: Protected Rights Obj.

Protected RO

Contents Encryption Key (CEK)

Permission

Digest of Content

Content ID

Digital Signature of Rights

Rights Encryption Key (REK) and MAC Key

MAC of RO

Encrypted Using REK (Symmetric Key)

Integrity Check for DCF

Authentication, Non-Repudiation, and Integrity Check for Rights

Encrypted Using Device’s Public Key

Integrity Check for RO (Including REK)
Domains

Acquired in Domain Joining

Right Issuer

Content Issuer

Send Domain ROs via ROAP

Contents Encrypted Using CEKs

All Devices That Have Joined the Domain Can Use Contents

Domain

Domain RO

Domain RO

Encrypted Content

Mobile Phone 1

Mobile Phone 2

PC

Notebook

User

MESLab, CSE, SNU