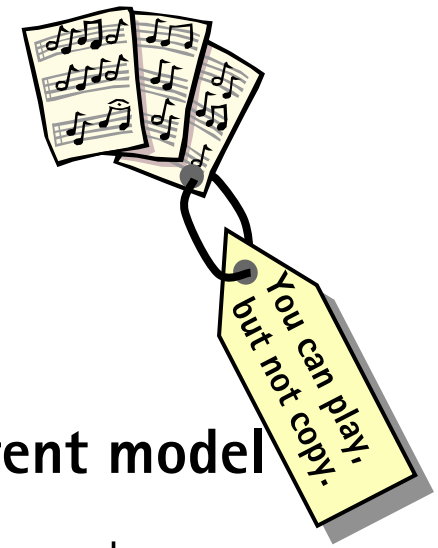
OMA DRM Overview

Digital Rights Management

- Controlling the usage of digital objects in cyberspace

1. Associate *usage rules* with digital content
2. *Enforce* that the rules are followed



- What we really want to do is to **enable the paid content model**
  - Content owner gets paid when his content is consumed
  - An alternative for the subsidized advertising model – banners suck
- **Superdistribution** is an important feature
  - Excellent content propagates from peer to peer like a virus – and the content owner gets paid for each copy

NOKIA

Threats and counter-measures

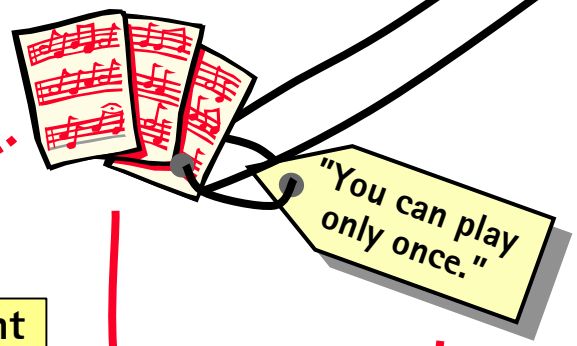
The challenge is not to *express* rights, but to *enforce* them.

NOKIA

Threats

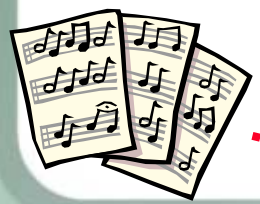
Content

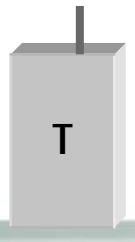
- A Mickey Mouse screensaver



Replace content with illegal one

Extract content from the DRM system





Replace the rights with more loose ones

Rights

- Enable preview (test drive)

```
<rights>
   <agreement>
      <asset>
         <uid>mid:mickey_14@disney.com</uid>
      </asset>
      <permission>
         <play>
            <count> 99 </count>
         </play>
      </permission>
   </agreement>
</rights>
```

Modify the existing rights

Terminal

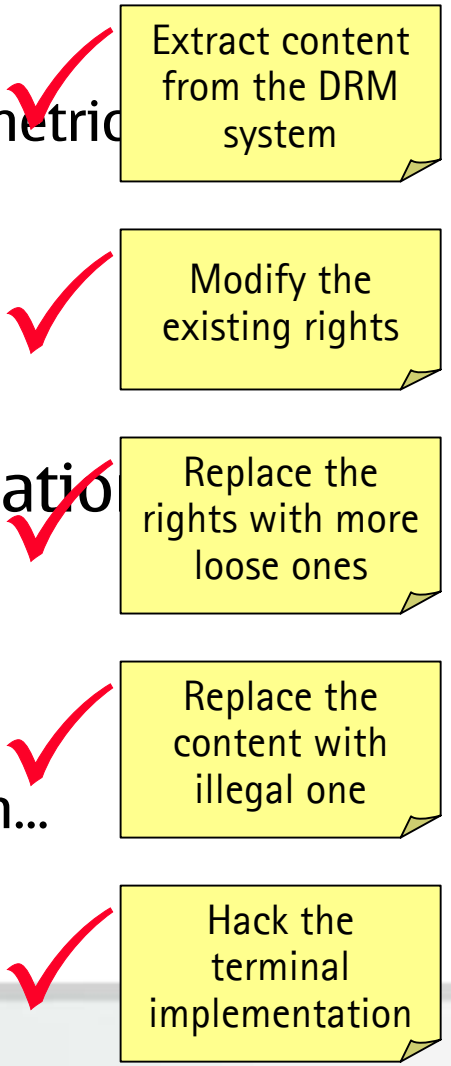
- Plays the content **forever**

Hack the terminal implementation

NOKIA

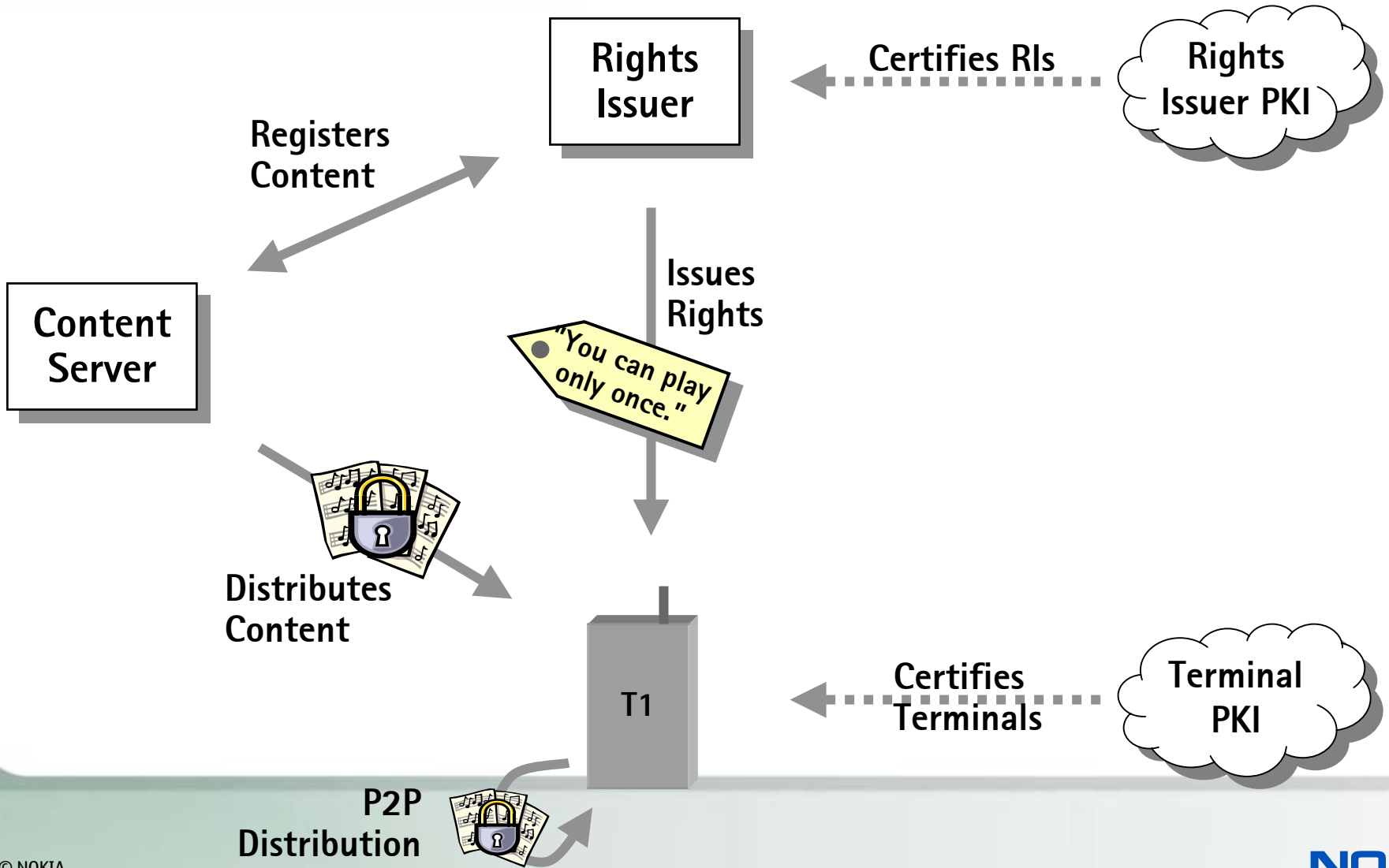
Counter-measures

- Protect the confidentiality of Content
  - *Content encryption*
  - In practise hybrid encryption i.e. combination of symmetric and asymmetric encryption
- Protect the integrity and authenticity of Rights
  - *Digitally signed Rights*
- Protect the integrity of the Content-Rights associatio
  - Include *hash of the content* inside the (signed) Rights
- Careful implementation inside the terminal
  - Access control, integrity and confidentiality protection...
  - Only well behaving applications shall be able to access the bits



NOKIA

Example architecture



Implications

- Key management infrastructure – actually maybe even two
  - Terminal PKI – content encryption, device authentication
  - Rights Issuer PKI – signed rights
- Both Terminal and Rights Issuer have a private key to hide
  - Hiding secrets is difficult – especially in the DRM threat model
- The counter-measures are not cheap
  - Computationally expensive, increased footprint, deployment issues
  - Overkill for low value content
- The market needs something that can be deployed now !

OMA DRM Rel 1 Simplifications

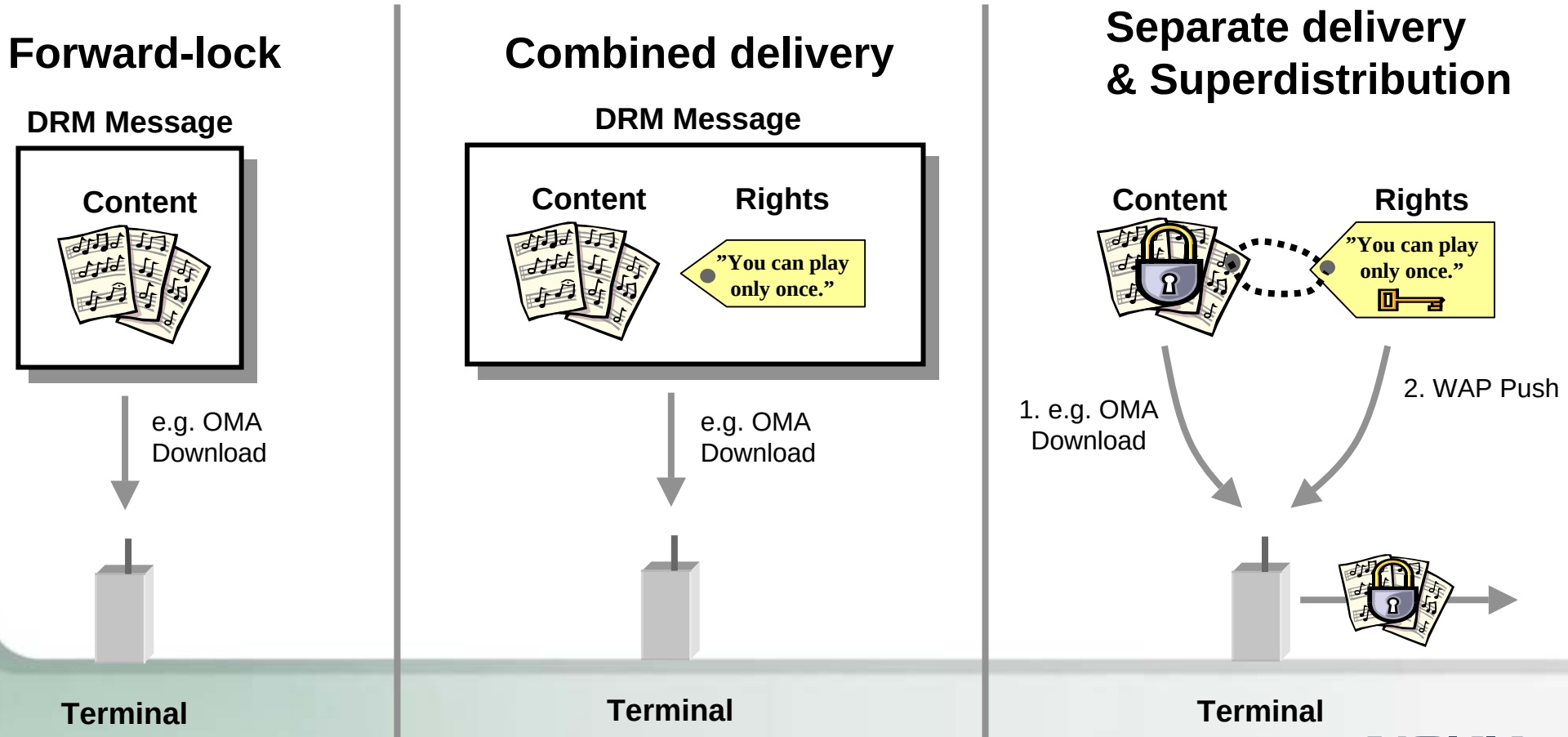
1. Forget the key management infrastructures
   - No Terminal or Rights Issuer PKIs
     - No private keys / trust roots in terminals
     - No private keys / trust roots at Rights Issuers
   - Big trade-off between security and simplicity / ease of deployment
2. No DRM-specific architectural entities
   - No DRM-servers
   - Rights Issuer = Content / rights packaging tool
   - Easy to deploy
- However, an evolution path towards a “real DRM” should exist
- Functional requirements:
  - Object level “forward-lock” semantics
  - Preview feature

OMA DRM Rel 1

”A simple DRM for low value mobile content”

How to deliver content and rights ?

- OMA DRM Rel 1 defines three DRM methods



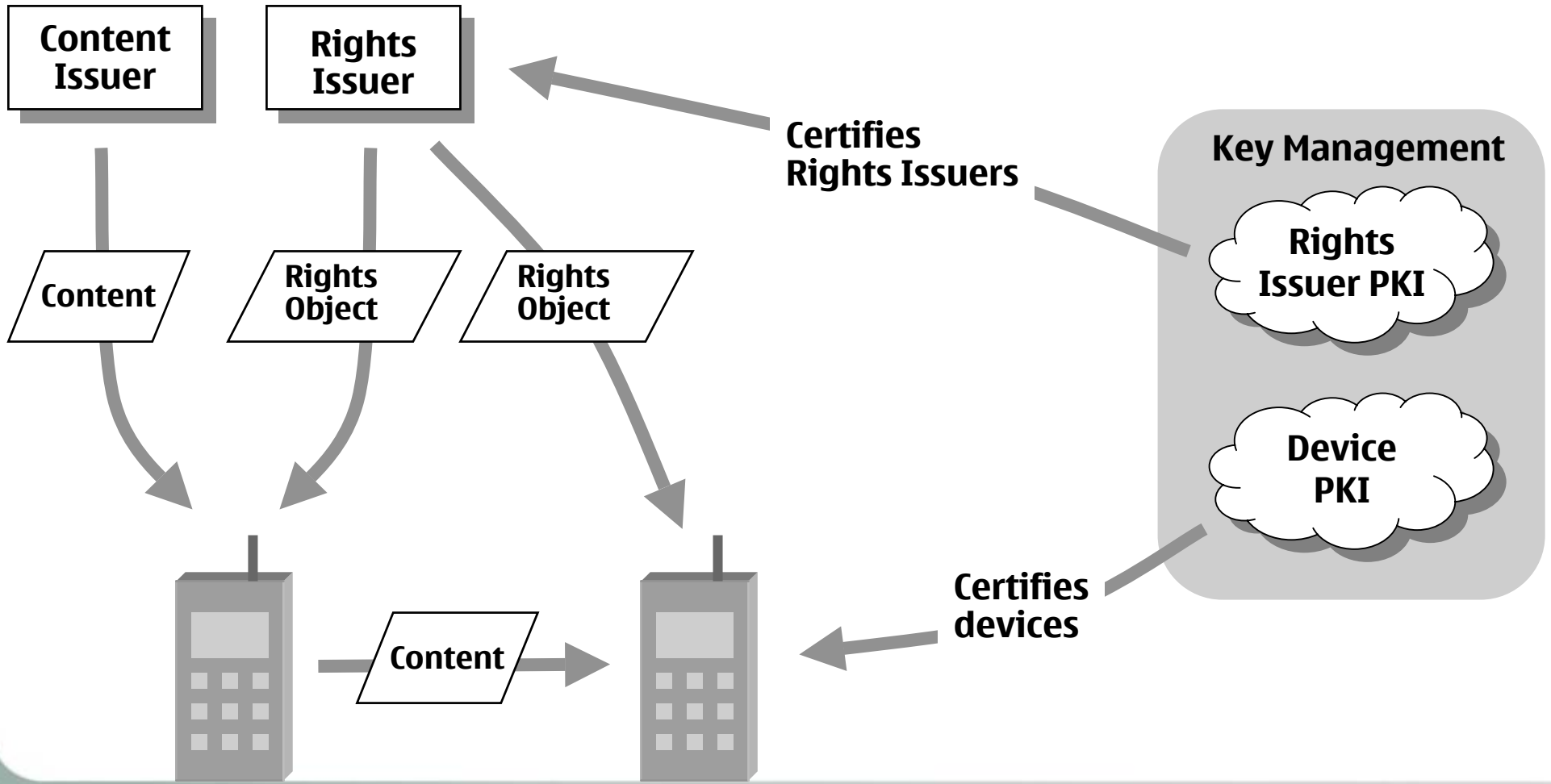
OMA DRM Release 2

OMA DRM Rel 2 Requirements

- Main requirement for OMA DRM Rel 2:
  - Need to support more valuable content => more security required
  - Music and video
- The two big assumptions that made life easy in OMA DRM Rel 1 go away
  - OMA needs to bite the bullet
- A key management infrastructure is needed to provide more security
- If we do have terminal keys we need to personalize the rights objects on-the-fly
  - In OMA DRM Rel 1 the same rights object can be sent to any terminal
  - In OMA DRM Rel 2 the service must encrypt parts of the rights object with a terminal specific key
  - A real-time back-end solution is needed to do that

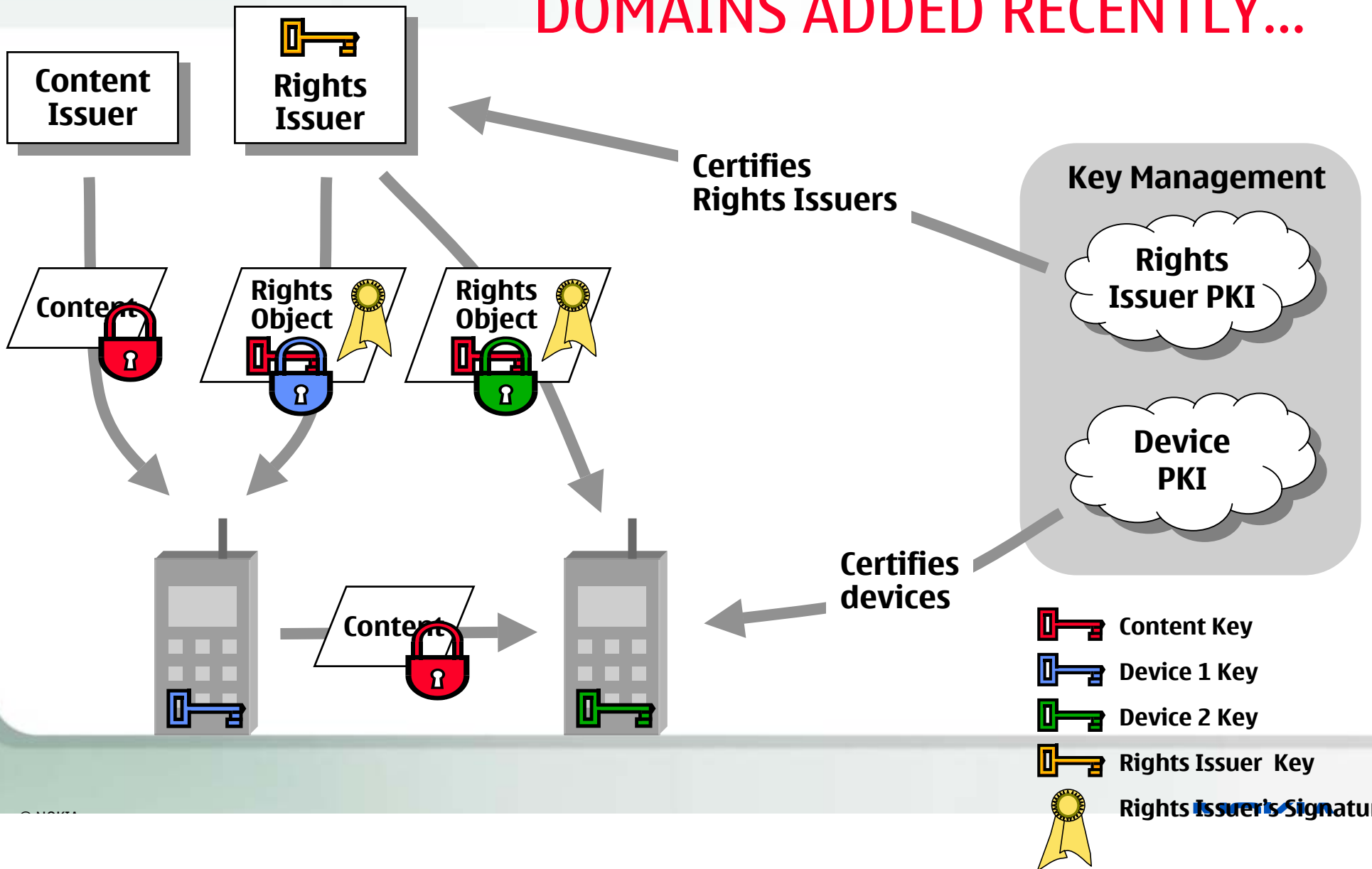
NOKIA

OMA DRM Release 2



OMA DRM Release 2

DOMAINS ADDED RECENTLY...

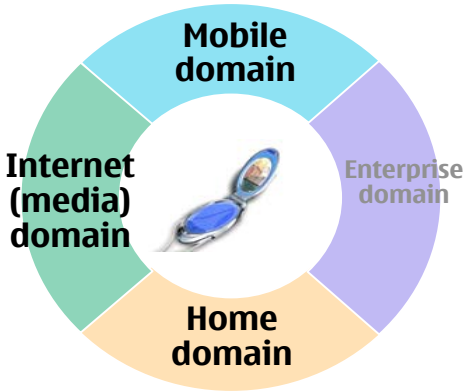


OMA DRM 2.0

Next generation open DRM technology specification

Fulfills security requirements of future rich media e.g. music services

Enables consumers to buy content once and consume with his/her registered devices



Convergence of DRM technology across Internet, media, mobile and home domains

NOKIA

Learnings and summary

- Most people conduct payment transactions practically every day and carry a mobile phone, too
  - It is a strong value proposition for consumers and merchants if some part of these payments could be conducted with a mobile phone
- Remote macro payments are increasing – existing credit card infrastructure offers a globally sustainable solution
- While today's technologies offer strong enablers, m-Commerce and mobile payments market is primarily business driven
- Practical DRM is needed today
- End-use experience is crucial: "easy to find, to use, to pay!"
- Sustainable value chains are essential for the expansion of m-Commerce and mobile payments ecosystem
- Co-creation of the customer experience is needed

NOKIA

CONNECTING PEOPLE

