

PHILIPS

Digital Rights Management and Privacy Protection

Milan Petković

Information and System Security Department

PHILIPS Research Laboratories

Joint work with Claudine Conrado and Willem Jonker



Overview

- Motivation - Privacy Issues in DRM
- A Privacy-Preserving DRM System
- Private Transfer of Licenses
- Privacy-Preserving License Management within an Authorized Domain
- Conclusions



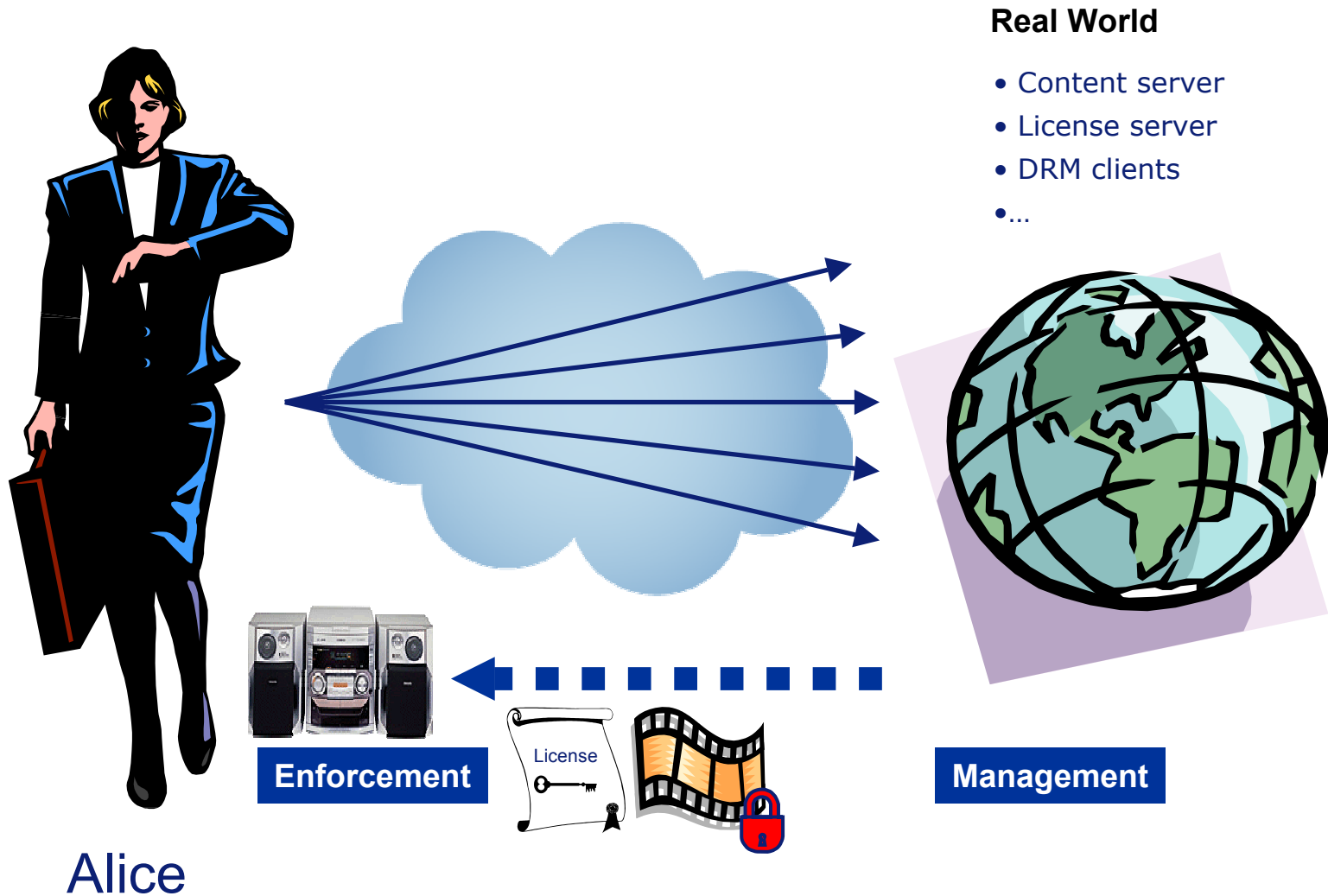
Motivation

DRM systems provide a means for protecting digital content, but at the same time they violate the privacy of users in a number of ways:

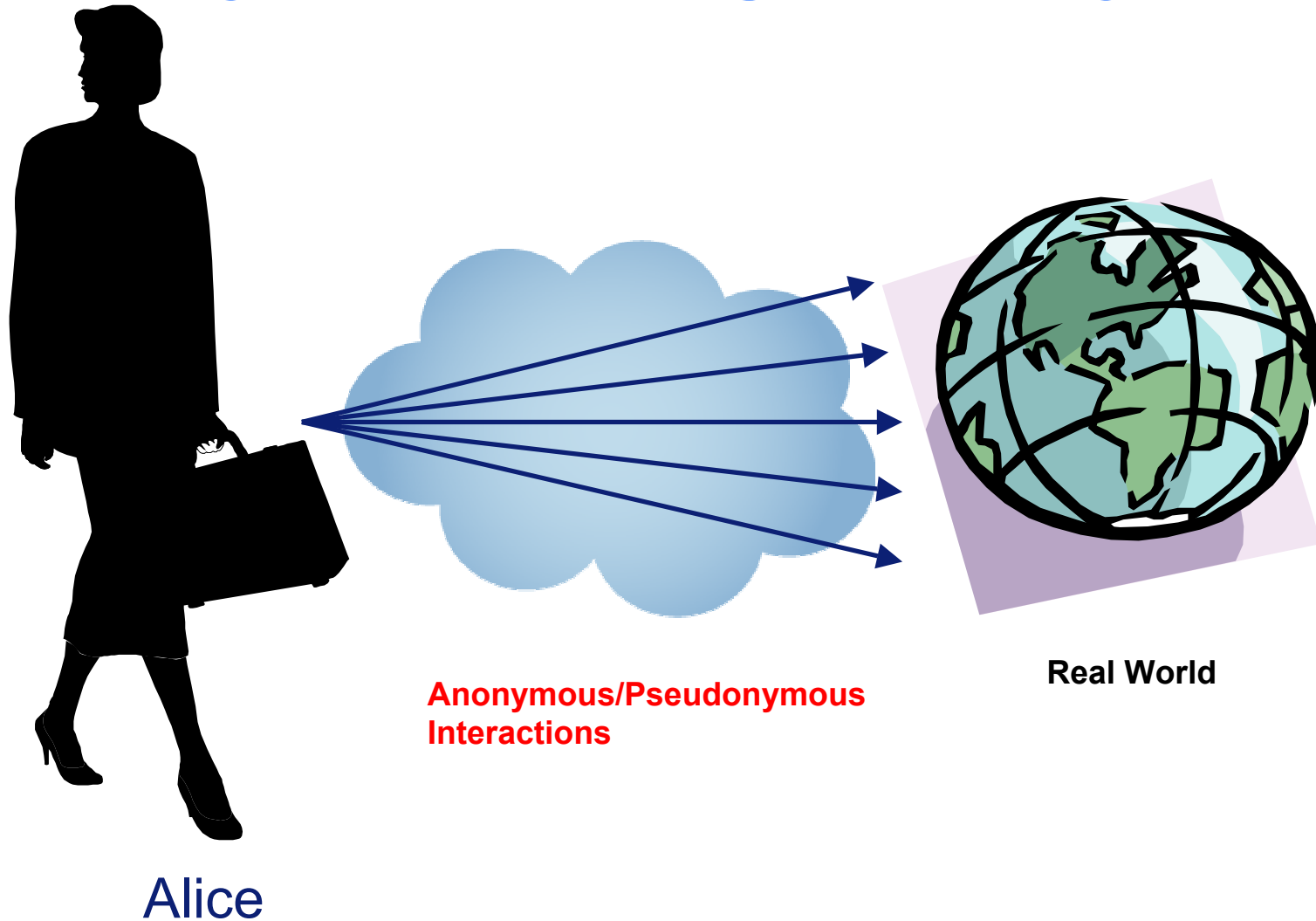
- usually do not support anonymous and un-linkable buying
- generally involve tracking of the usage of content in order to keep control over the content
- might collect information such as user identification, content identification, time, place, etc.

The main challenge is how to allow a user to interact with the system in an anonymous/pseudonymous way, while preserving all security requirements of usual DRM systems

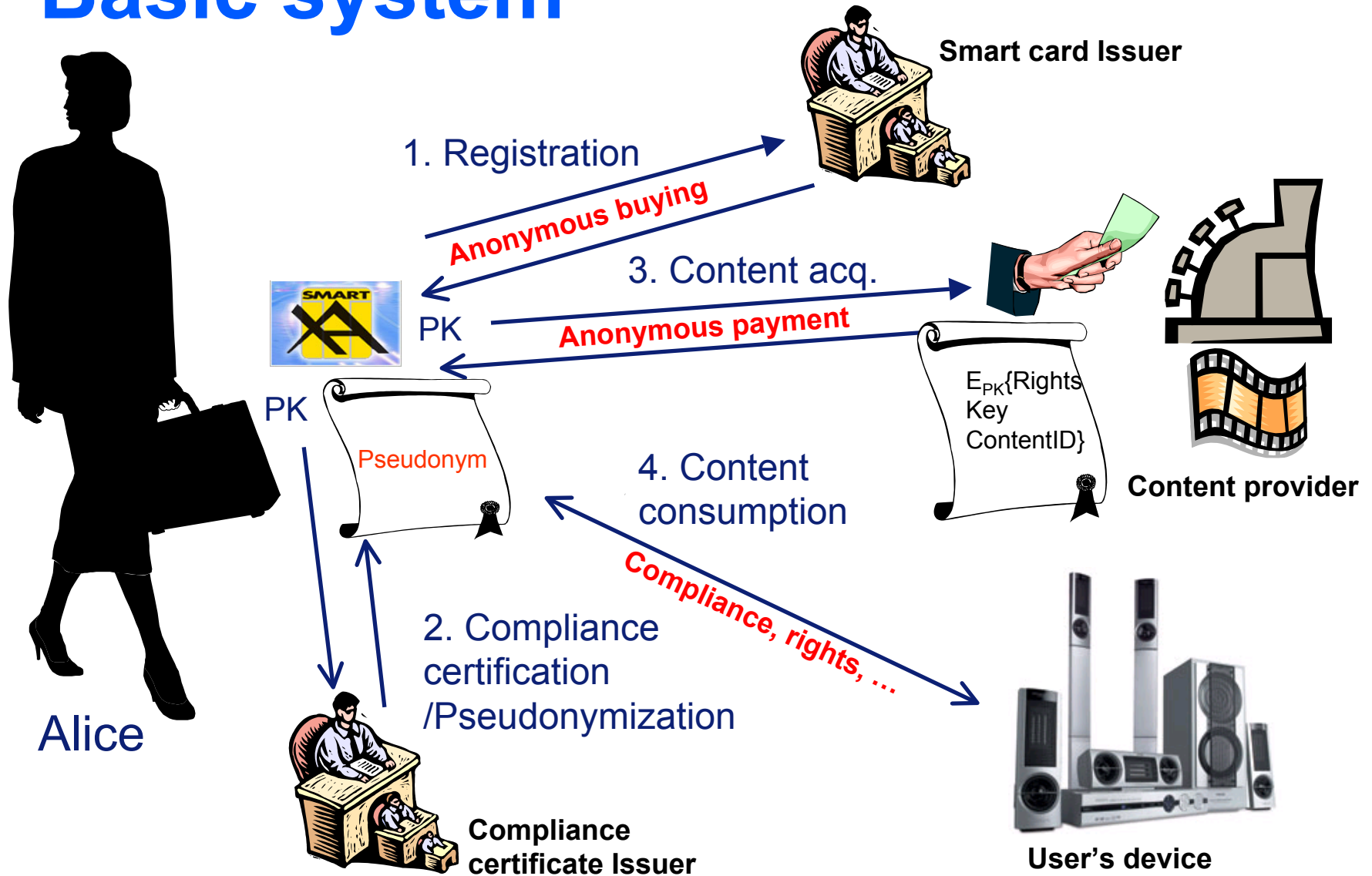
Privacy invasive DRM system



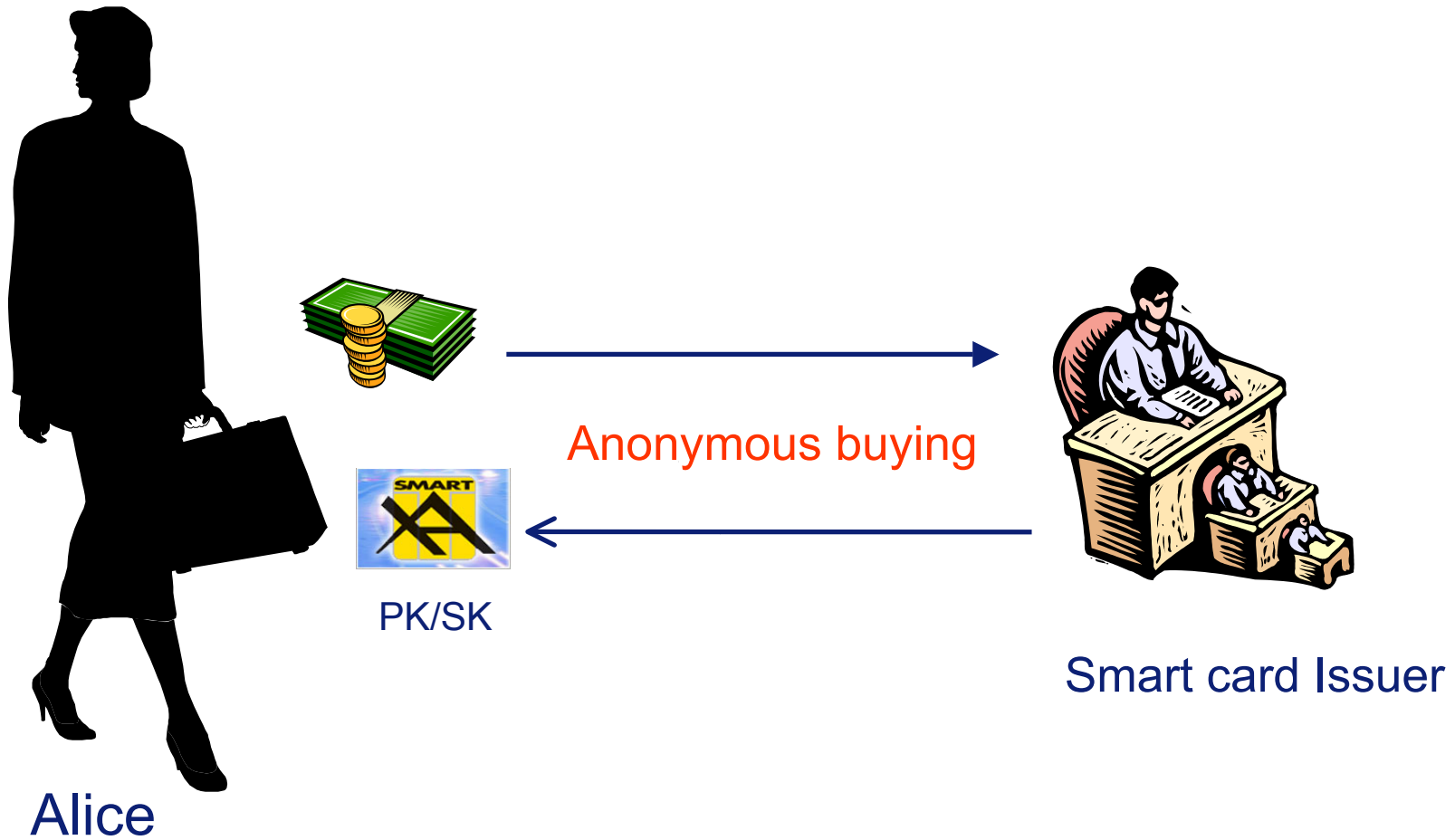
Privacy Preserving DRM system



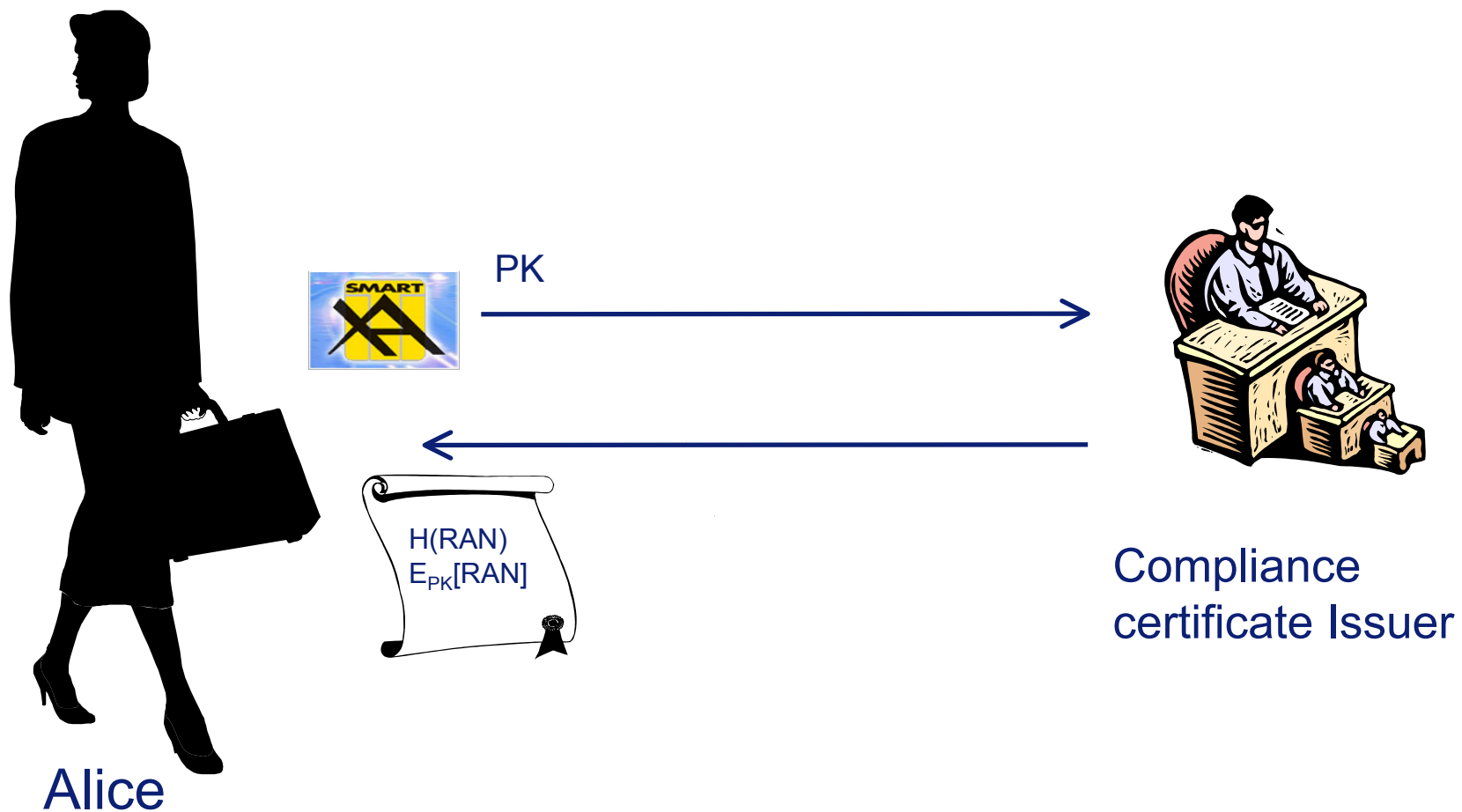
Basic system



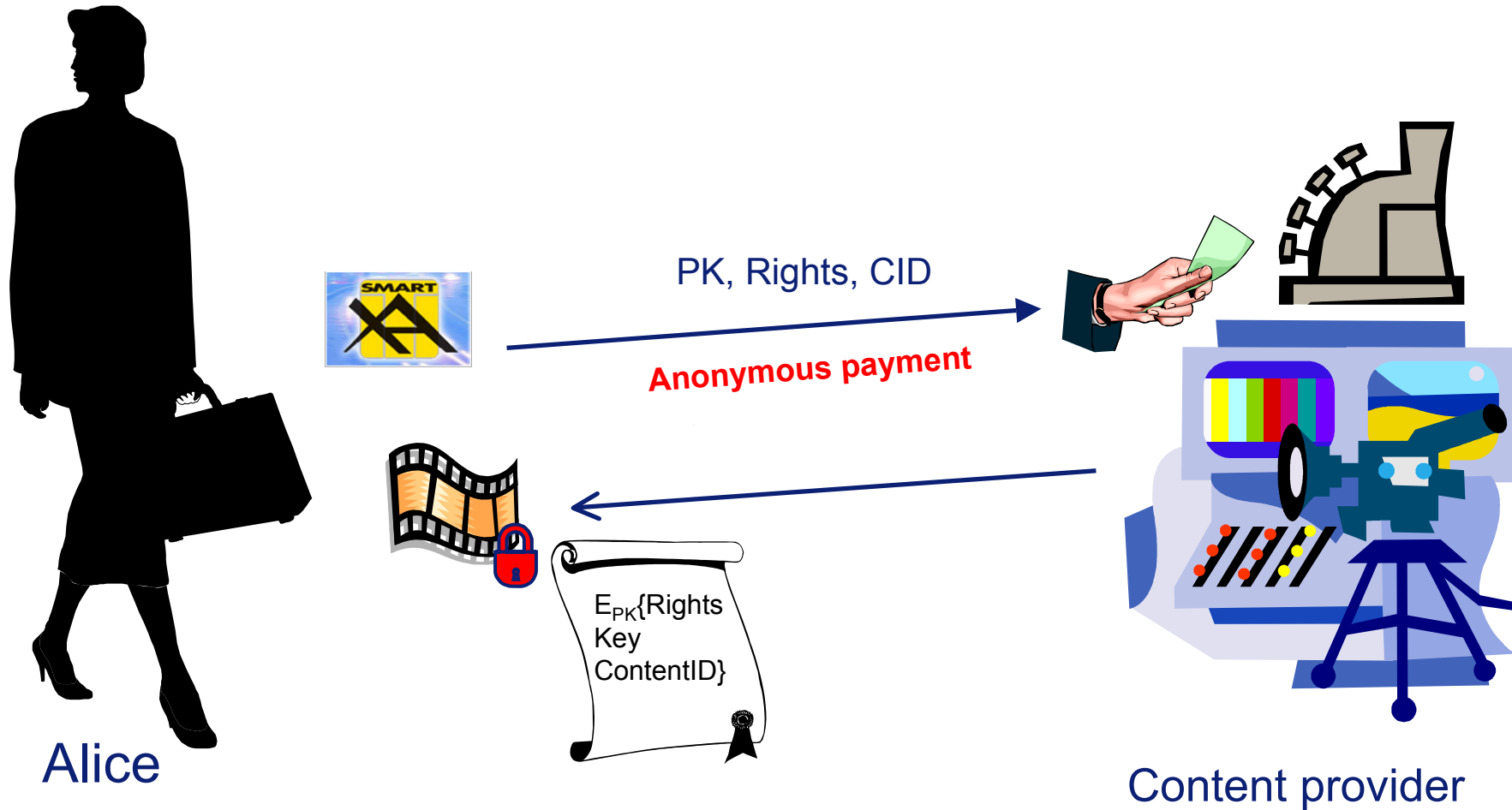
Registration



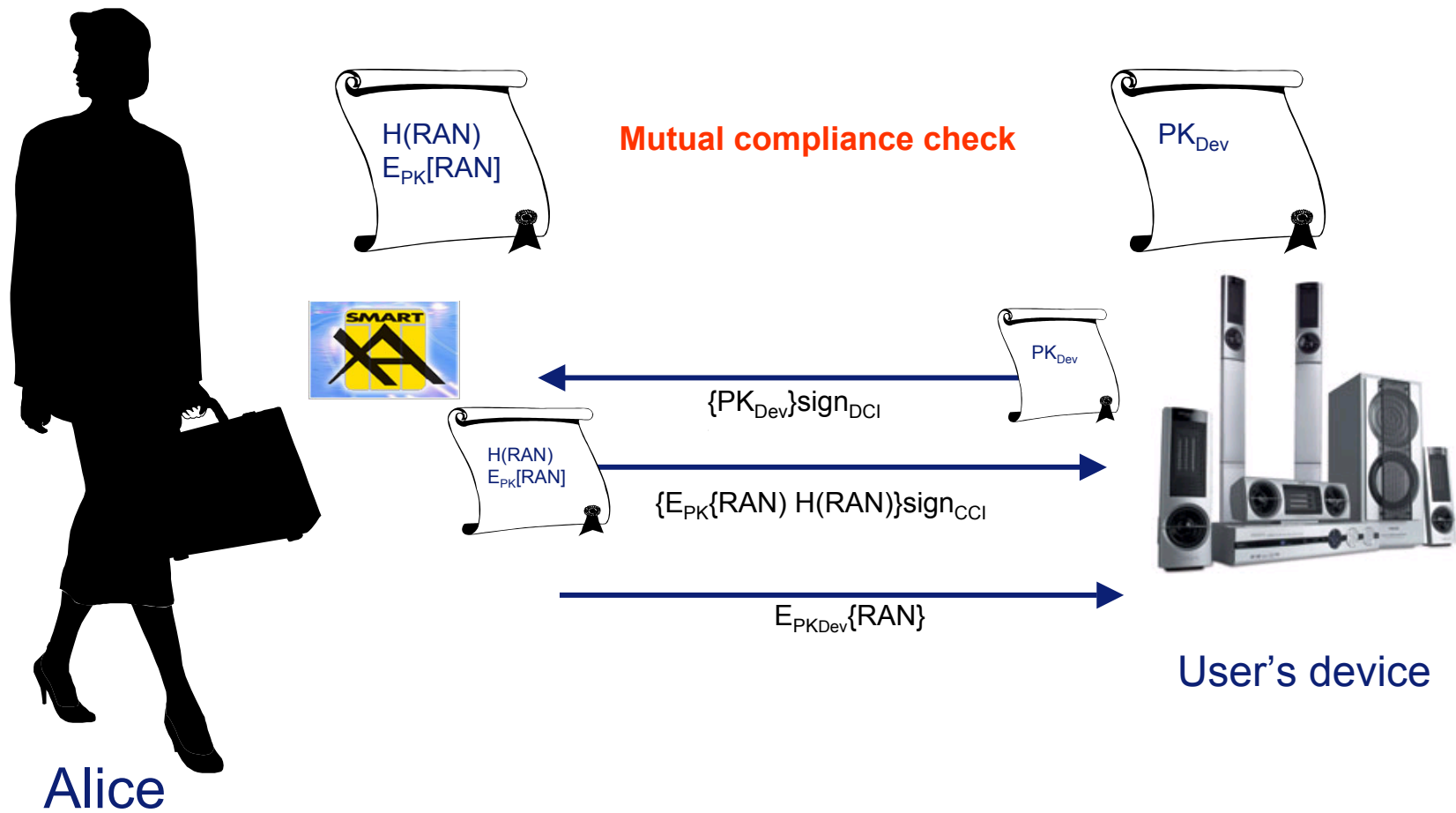
Pseudonymization



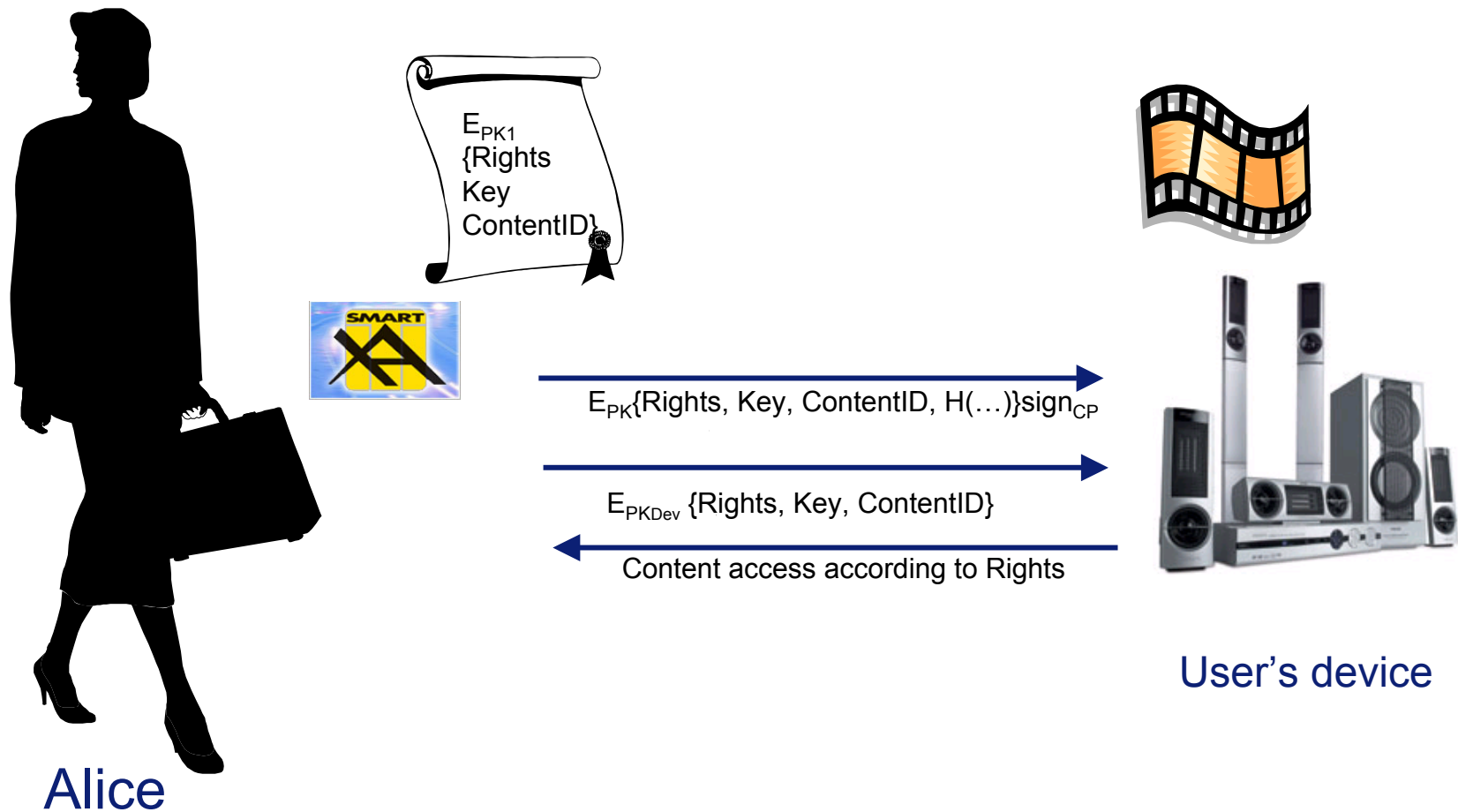
Content acquisition



Content consumption



Content consumption





Privacy Preserving DRM system

Features

- *Form of licenses $\{E_{PK}[Sym//Rights//ContentID], H(\dots)\}_{signCP}$*
- *The real identity of the user cannot be revealed*
- *Privacy and non linkability towards a public device*
- *If an attacker is able to obtain user-related information from the CoD after a content access transaction happens, he can create only the following associations:*

(real user identity \leftrightarrow RAN),

(real user identity \leftrightarrow (content, Rights, Sym))



Transfer of licenses



A straightforward approach to the transfer of licenses

- The first user contacts the CP, authenticates, presents the license to be transferred and the second user public key
- The CP revokes the old license, creates a new one and gives it to the first user
- The first user gives the new license to the second user

When the license is transferred from the first to the second user, the CP learns the association between those users!



Anonymous licenses

- The first user contacts the CP, authenticates, presents the license to be transferred
- The CP revokes the old license, creates an **anonymous license** and gives it to the first user
- The first user gives the anonymous license to the second user
- **The second user presents the anonymous license to the CP and personalize it.**



Anonymous licenses

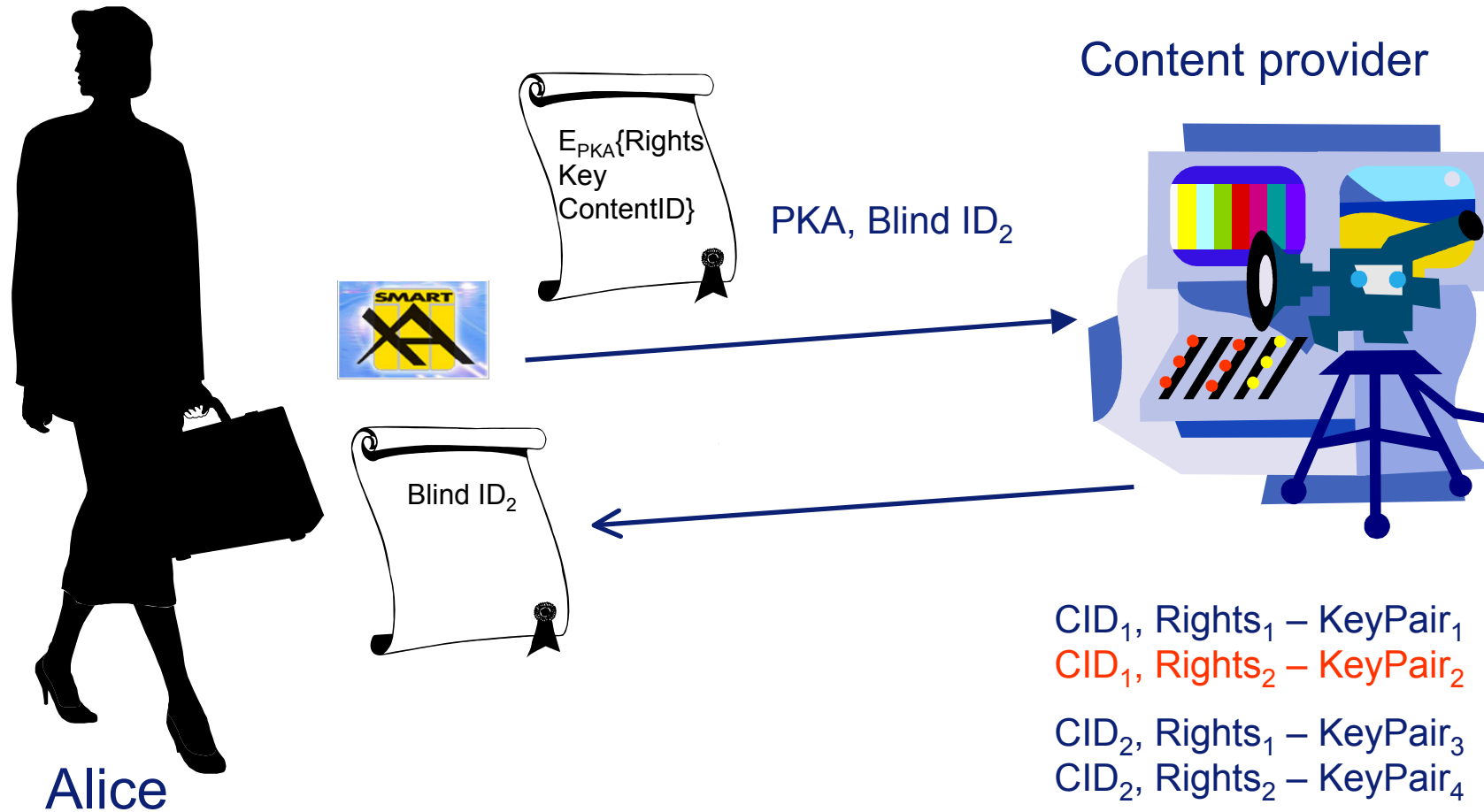
Requirements

- The CP shouldn't be able to link anonymous license with the first user PK
- The license specifies Rights and Content ID
- The anonymous license shouldn't be multiple redeemable

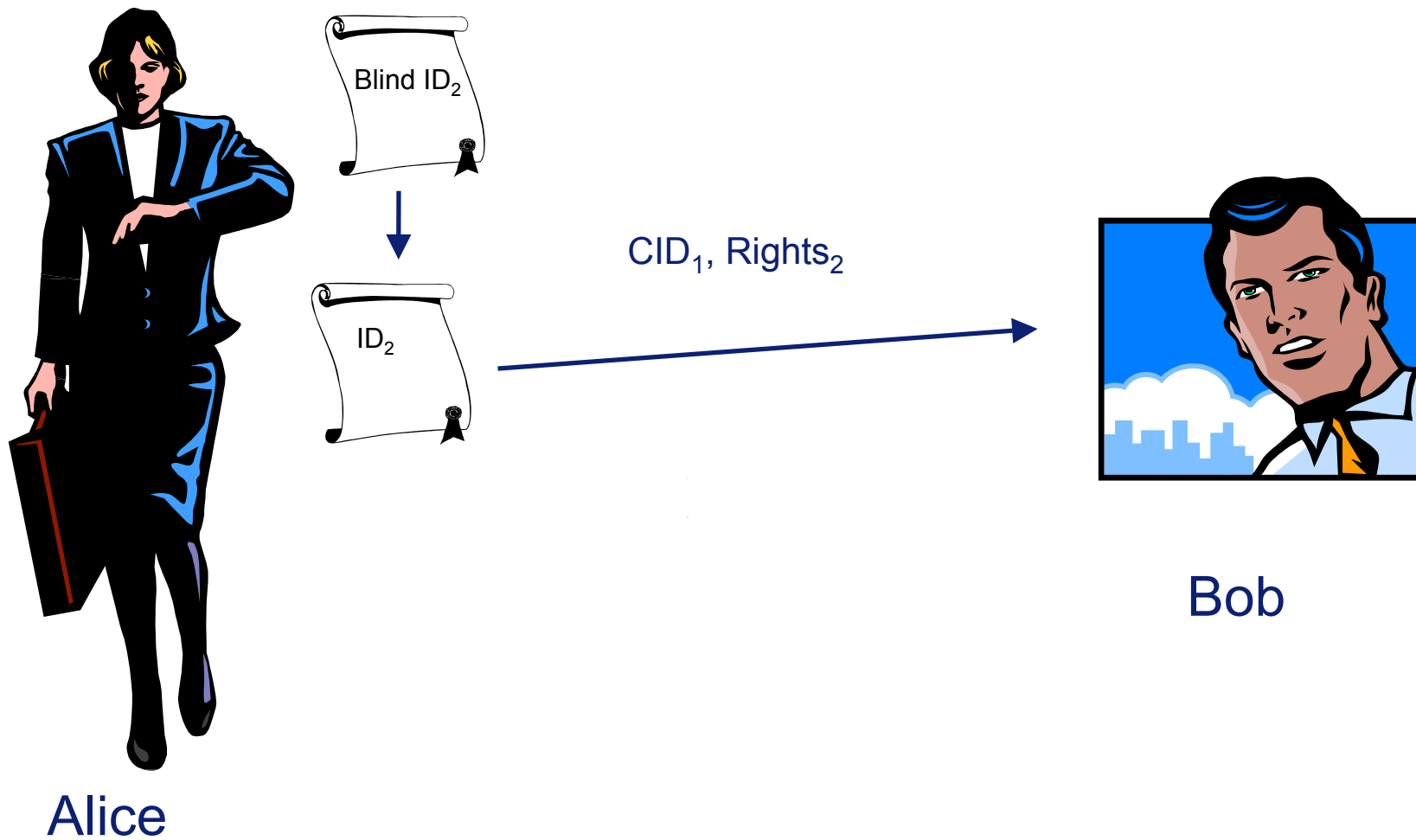
Approach

- The first user creates a secret random identifier ID, blinds this value and sends it to the CP
- The CP signs the license with a key that is unique per each combination of rights and content
- Unique ID prevents multiple redeeming
- Identity-based Cryptography for Key Management by the CP

Acquisition of a non-linkable license



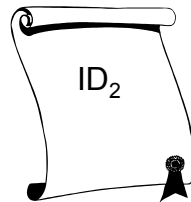
License transfer



Redeeming



Bob



PKB, CID₁, Rights₂



$E_{PKB}\{\text{Rights Key ContentID}\}$

Content provider



ID₁,
ID₂,
ID₃,
...

CID₁, Rights₁ – KeyPair₁
CID₁, Rights₂ – KeyPair₂
CID₂, Rights₁ – KeyPair₃
CID₂, Rights₂ – KeyPair₄



Some details (implementation with the RSA scheme)

Key generation

- p, q large primes; $n=pq$; $\phi = (p-1)(q-1)$; select e : $1 < e < \phi$, $\gcd(e, \phi) = 1$; compute d : $1 < d < \phi$, $ed \equiv 1 \pmod{\phi}$
- Public key (n, e) ; Private key d

Protocol

- Alice select a random value k : $\gcd(n, k) = 1$
- Alice blinds ID : $m^* = IDk^e \pmod{n}$ and sends m^* to the CP
- The CP signs it: $s^* = (m^*)^d \pmod{n}$ and returns s^* to Alice
- Alice un-blinds it: $s = k^{-1}s^* \pmod{n}$ and obtains signature s on message ID

$$s = k^{-1}(IDk^e)^d \pmod{n} = ID^d \pmod{n} = s$$



Privacy-Preserving License Management within a Domain



Privacy-Preserving License Management

Features we would like to achieve:

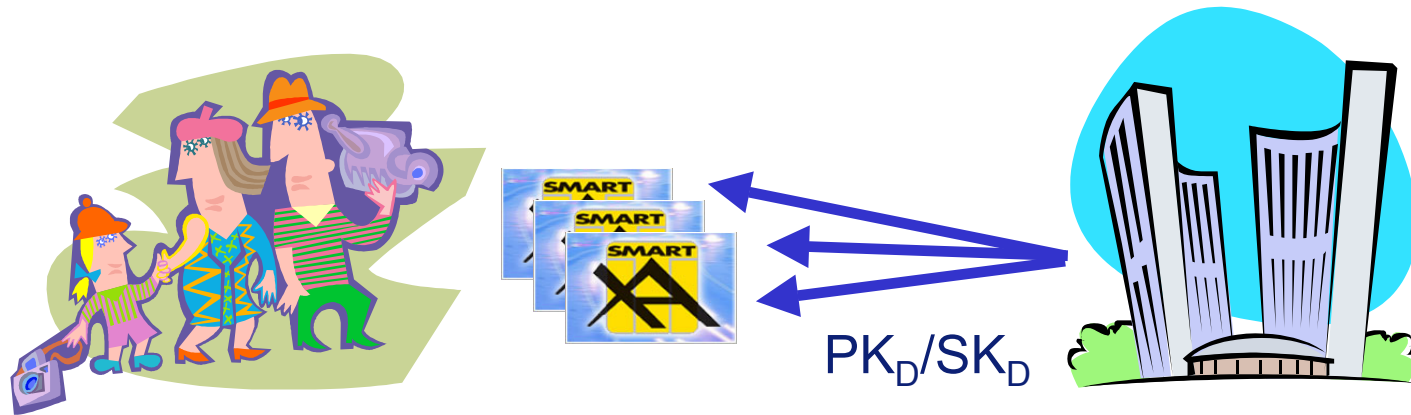
- Authorized Domain
- Different users - different rights for the same piece of content within a domain
- Private structure of the domain
- Privacy-preserving management of countable rights

Approaches:

- Preserving the structure
- Allowing different rights
- Preserving the structure and different rights

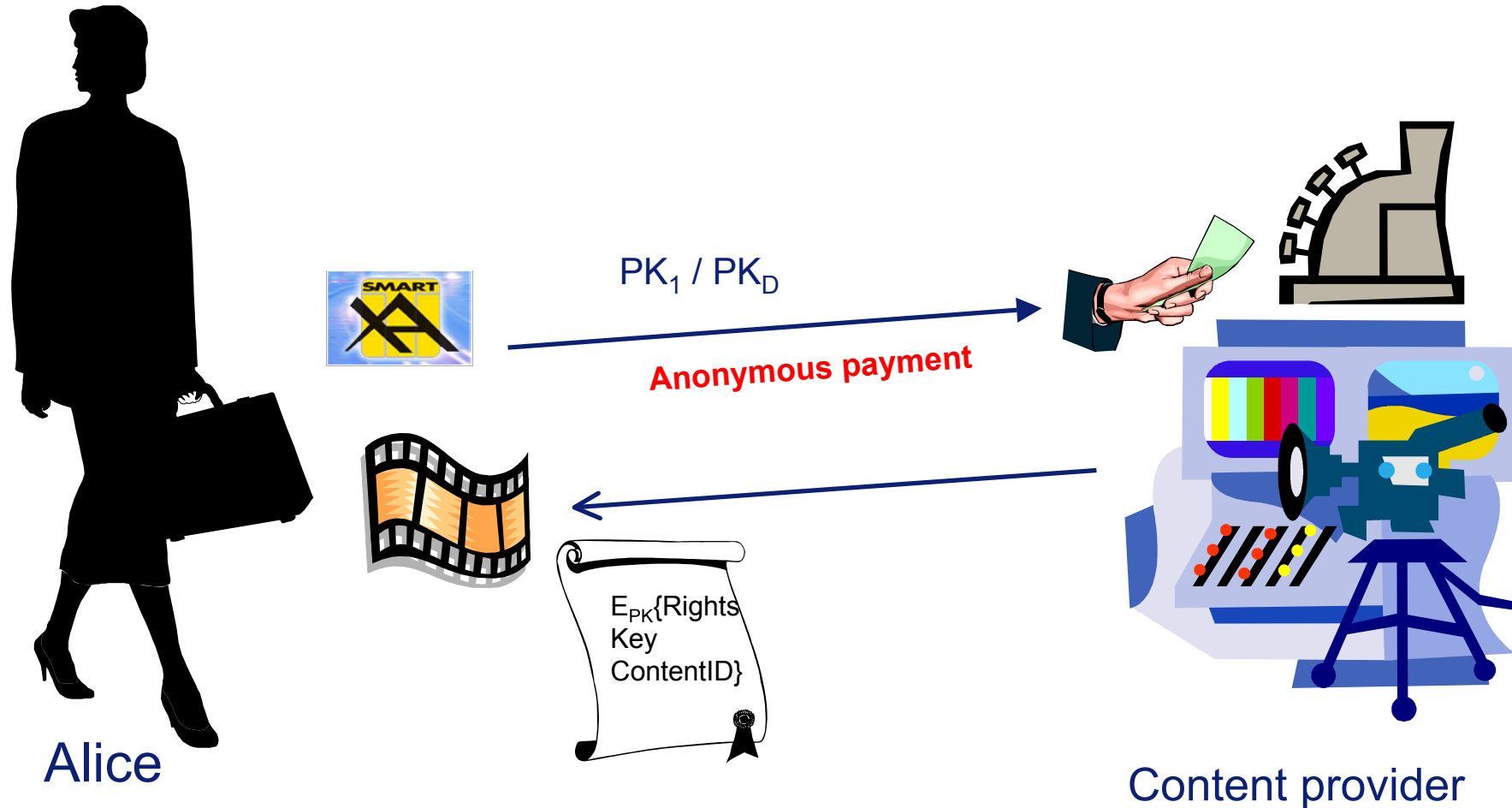
Domain with PK_D

Domain Registration



PK_D/SK_D : domain public-private key pair
 PK_1/SK_1 : personal public-private key pair

Content acquisition





Domain with PK_D

Domain Registration

Pros:

Privacy towards the CP for the domain structure: YES - the CP does not learn the structure of the domain

Simple to implement

Cons:

Rights differentiations within the domain: NO – it is black and white: no different rights for different domain members (all members have the same rights as the user who has bought the content, or all others have no rights)

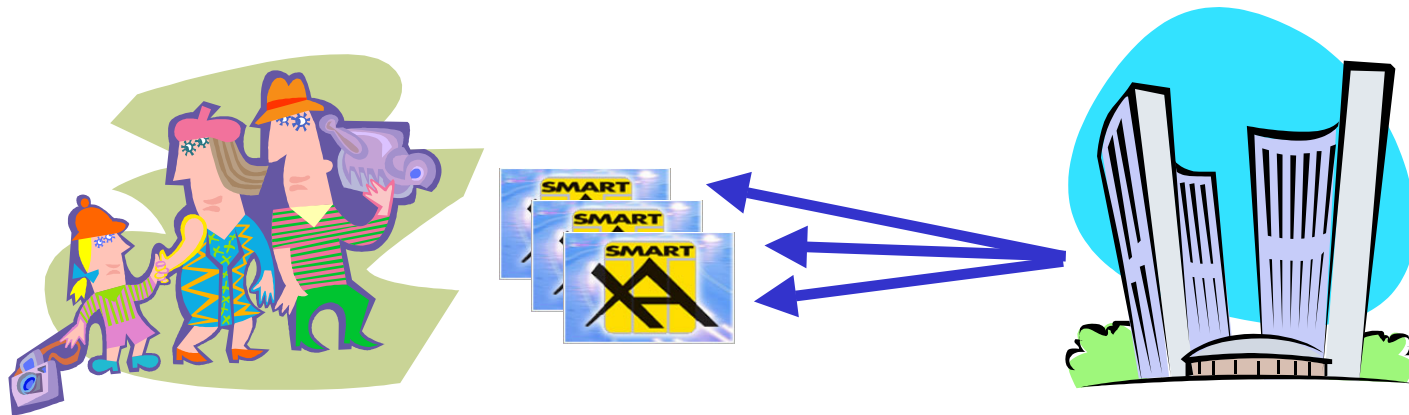
Behavioural privacy towards the CP for the countable rights problem: NO – CP knows the time, content, device, and user's PK for each user action that involves changing of countable rights

The solution for countable rights revocation is not appropriate: it is too late to include revocation list when the user go to CA-SC for a new RAN (until that he can copy content n times instead of only once)



Domain with different rights

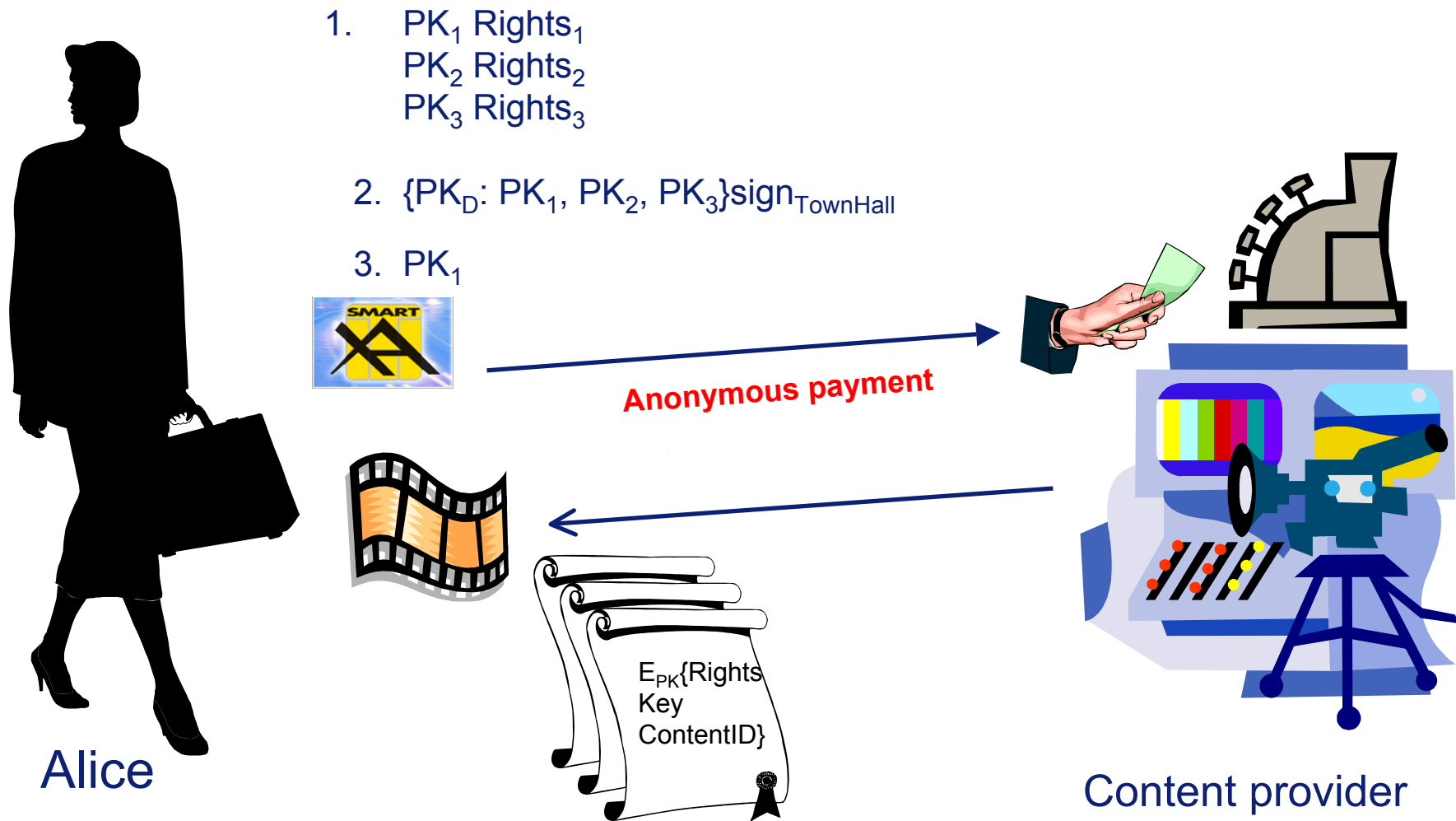
Domain Registration



$\{PK_D: PK_1, PK_2, PK_3\}sign_{TownHall}$

$\{PK_D: PK_1, PK_2, PK_3\}sign_{TownHall}$ - domain certificate

Content acquisition





Domain with different rights

Domain Registration

Pros:

Rights differentiations within the domain: YES - Different rights for different domain members

No extra key (PK_D)

Cons:

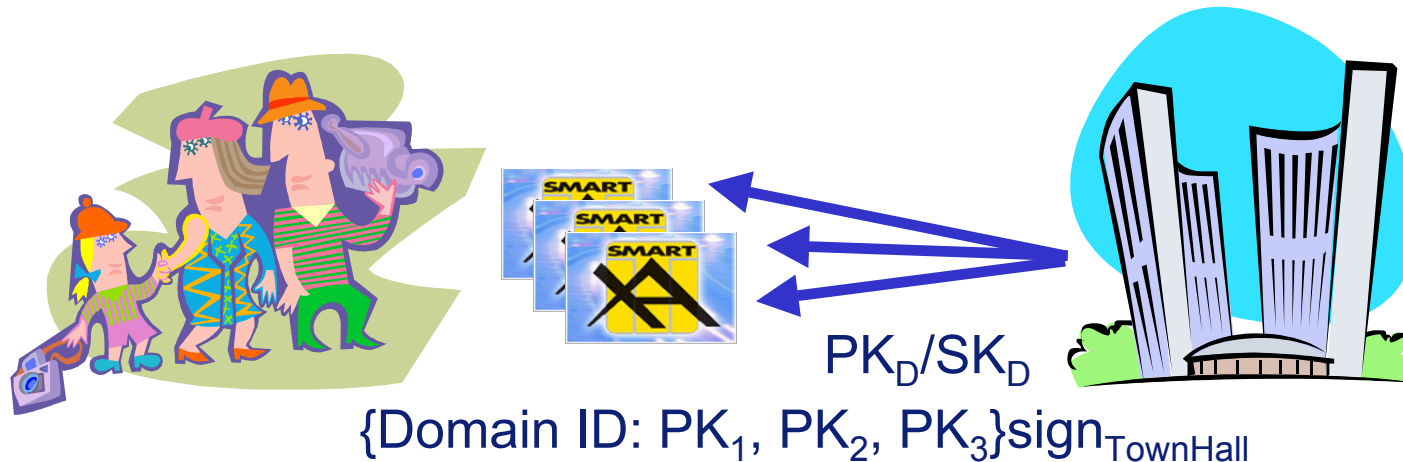
Privacy towards CP for the domain structure: NO - CP learns the structure of a domain (not the real user identities, but PKs which form a domain). This can be used for advertisement, spam, etc.

Behavioural privacy towards the CP for the countable rights problem: NO – CP knows the time, content, device, and user's PK for each user action that involves changing of countable rights

The solution for countable rights revocation is not appropriate: it is too late to include revocation list when the user go to CA-SC for a new RAN (until that he can copy content n times instead of only once)

Domain with PK_D and different rights

Domain Registration

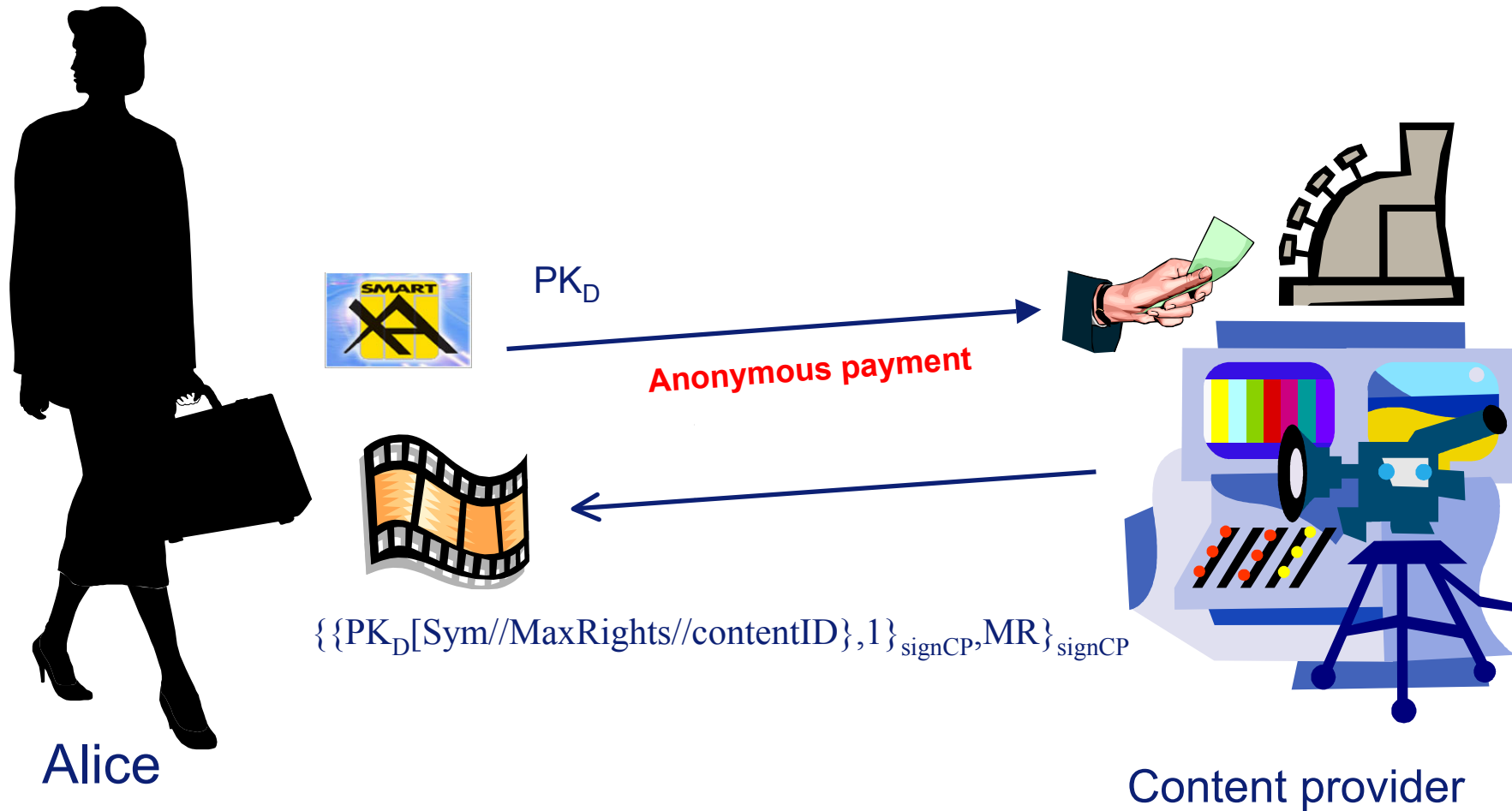


PK_D/SK_D : domain public-private key pair

PK_1/SK_1 : personal public-private key pair

{ $PK_D: PK_1, PK_2, PK_3$ } $sign_{TownHall}$ - domain certificate

Content acquisition



Creating individual licenses



Alice

1. PK_1 Rights₁
 PK_2 Rights₂
 PK_3 Rights₃
2. $\{PK_D: PK_1, PK_2, PK_3\} \text{sign}_{\text{TownHall}}$
3. $\{\{PK_D[\text{Sym} // \text{MaxRights} // \text{contentID}], 1\} \text{sign}_{\text{CP}}, \text{MR}\} \text{sign}_{\text{CP}}$



$\{PK_D[\text{Sym} // \text{MaxRights} // \text{contentid}], 1\} \text{sign}_{\text{CP}},$
 $\{PK_i[\text{Sym} // \text{Rights}_i // \text{contentid}], PK_{\text{DM}}\} \text{sign}_{\text{DM}}$



Domain manager device



Content consumption



Bob



$\{PK_D[Sym//MaxRights//contentid], 1\}sign_{CP},$
 $\{PK_2[Sym//Rights_2//contentid], PK_{DM}\}sign_{DM}$



Content



Device



Domain with PK_D and different rights

Domain Registration

Pros:

Rights differentiations within the domain: YES - Different rights for different domain members

Privacy towards CP for the domain structure: YES - CP doesn't learn the structure of the domain

Behavioural privacy towards the CP for the countable rights problem: YES
– CP cannot learn the time, content, device, and user's PK for each user action that involves changing of countable rights

The solution for countable rights revocation is OK as licenses are revoked instantly

Complexity: One more license and certificate, but CP has much less work (domain rights are issued by the DM, revocation is also done by the DM)



Conclusions

In the basic system, user privacy is achieved by decoupling the real user identity from his identifiers, namely PK and RAN, in the DRM system

Furthermore, when accessing a public device the user does not disclose his PK but only temporary pseudonym RAN, so if an attacker is able to obtain user-related information from the CoD after a content access transaction happens, the privacy damage is minimal

Concerning the transfer of licenses between users and regarding the distribution of licenses to domain members, the solutions proposed also guarantees the security of the DRM system and the privacy of the user

“Privacy-Preserving DRM”, in *Secure Data Management*, Jonker, Petkovic (Eds) LNCS 3178, Springer, 2004

