



A Case for Person-centric Digital Rights Management

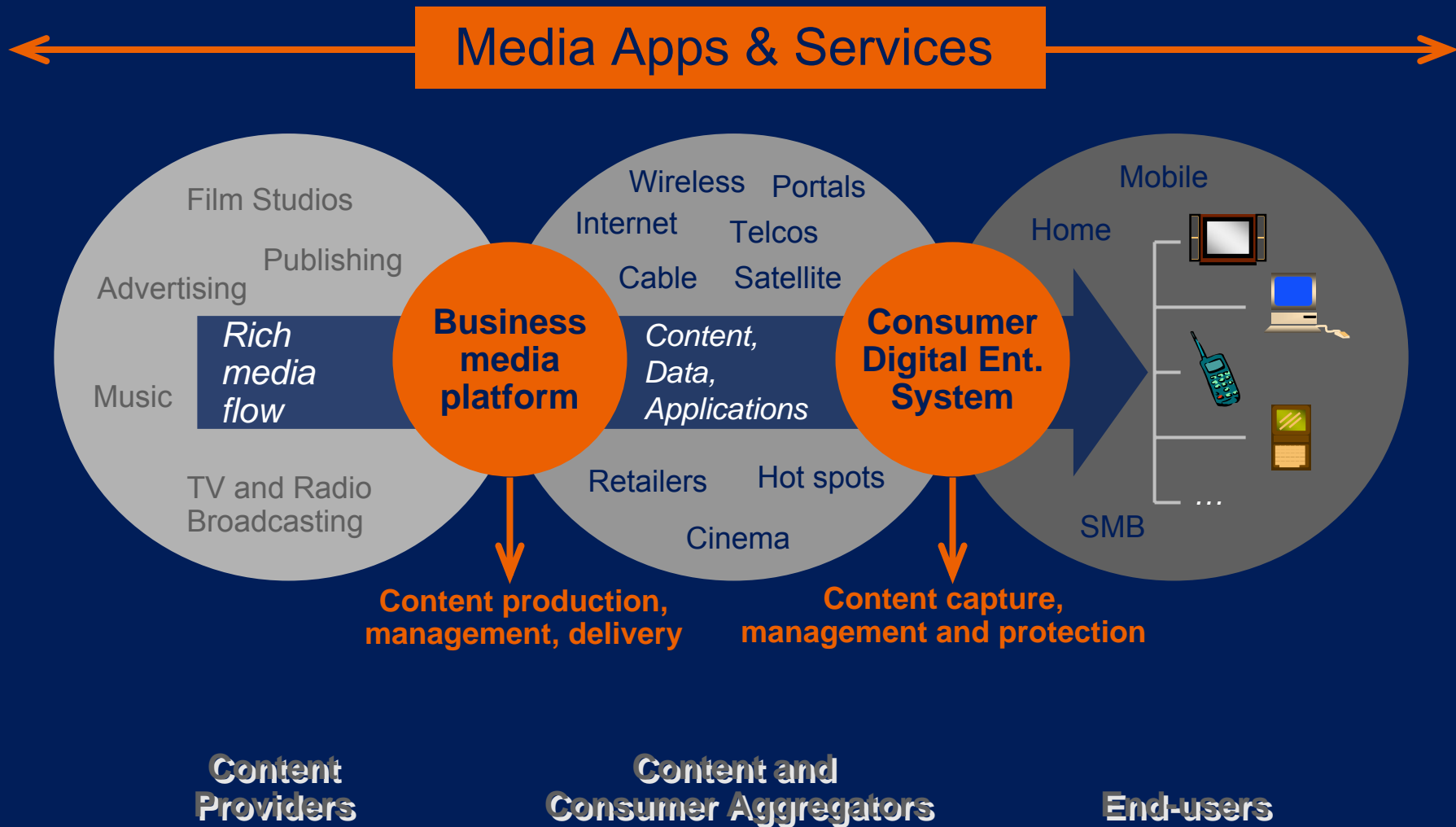
Ton Kalker, Mirjana Spasojevic, Amir Said,
Adam Petruszka, Pallavi Shah, Paul
Mclean

Hewlett-Packard, Palo Alto, CA

© 2004 Hewlett-Packard Development Company, L.P.
The information contained herein is subject to change without notice



Media production, distribution and consumption



Summary



Problem statement

- Current DRM systems (e.g. MS Janus, Real Helix, OMA_DRM, Apple FairPlay) are **device centric**
 - Enforcement and control is associated with device
 - Association between user and content is secondary
 - Limits on the number of devices that can play content
 - No mechanism to transfer licenses between devices

Proposed solution

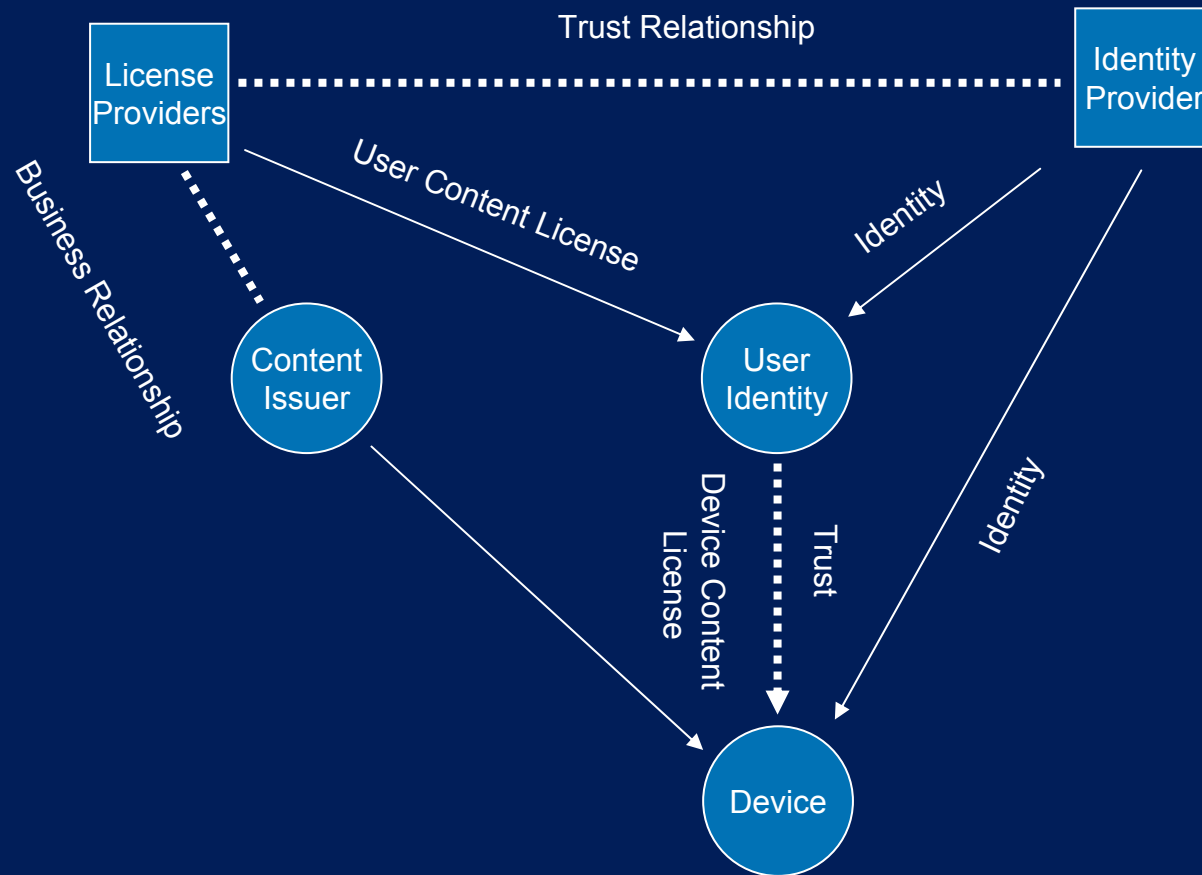
- **Person-centric** DRM system can rise above these limitations
 - Binding rights-objects (ROs) to users
 - Devices are anonymous rendering entities
 - Users interact with rights issuers; transfer of the license to a compliant rendering device is under control of the user
 - Enabling access to content **at any time, on any device**
 - Opportunity for distribution of licenses to groups of users

Basic Assumptions



- Basic philosophy is that Content Licenses (CL) are bound to an identity U (typically a user or a group of users), and that Content (CI) can be consumed on any device that is authorized to be associated to that identity U and with which the CL is compatible.
 - A device is regarded as an anonymous entity that assists the identity in consumption of the content
- A Personal Entertainment Domain (PED) is the dynamic collection of
 - A User Identity, representing a single or group of person(s) U (static);
 - Any number of content licenses CL_i, bound to the identity U (semi-dynamic);
 - Any number of devices (fully dynamic)
- Identities (be it for a User, Device or Content License) are globally unique
- Devices are transient members of multiple PEDs
- Licenses (CL) are assigned to identities, not devices

Participating Entities



User Identity



- A User Identity is a non-empty group of basic (atomic) User Identities
 - same mechanisms for broadcast (large groups) and ‘authorized domains’ (small groups; family)
- Any User Identity is able to compute from its internal secrets a secret binding private key
 - this process of private key generation does not reveal any internal secret to any User Identity
 - the Identity provider is able to compute the public key for any User Identity
 - Users are able to form ‘domains of users’ on the fly
- Any member of a User Identity is able to read and process licenses targeted for that User Identity
 - any non-member cannot not.
- Personal token for authentication of a user to a device (DRM agent)

Device Entity



- A device entity is characterized by
 - an identity provided by an IPr
 - a set of capabilities
- A device may associate to a user
 - mutual authentication
 - mostly dynamic
 - under the control of the ‘owner’ of a device
- The owner of a device
 - is static association between user and device
 - singleton (but user may have several members)
 - sets rules for other users to associate
 - may transfer ownership to another user
- Device may accept device content licenses
 - rules and regulations for rendering content
 - derived from user content licenses
 - consumption under the control the issuing user

License Provider



- A License provider provides User Content Licenses (UCL) to User Identities, either upon request or self initiated.
- A Content License contains and specifies
 - An ID of the requested Content Item (CID)
 - An ID of the targeted User Identity (UID)
 - This might be a sub-user of the requesting User Identity (LPr Policy)
 - Digital Rights for CID
 - allowed rendering rules
 - limits on states (e.g. play counts)
 - allowed rendering devices
 - Cryptographic keys for unlocking Content
 - MAC
 - LPr certificate
- A content license is encrypted with the public key of the UID
 - consumption only allowed by targeted UID

Device Content License

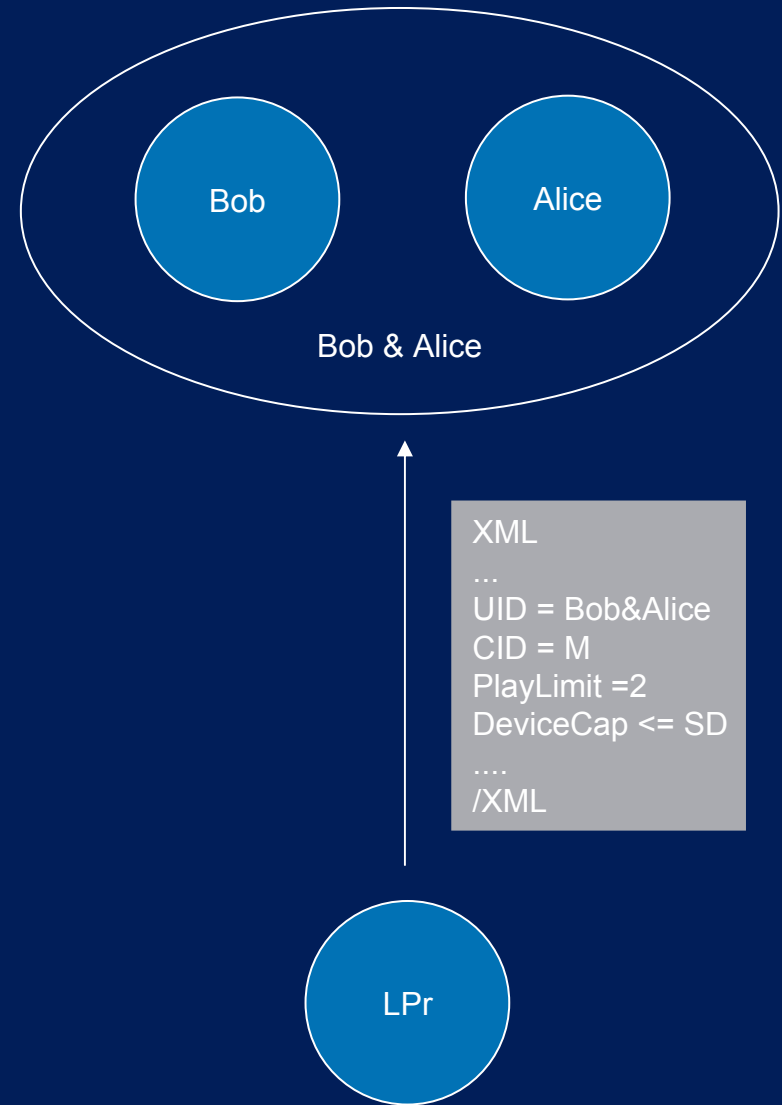


- A Content License can be transferred to an associated device DI
 - Device Content License (DCL)
 - Only members of the UID in the DCL may execute the DCL
- The DCL is derived from the UCL
 - DCL rights may be a proper subset of UCL rights
 - UCL rights may be forced to update with DCL delivery
 1. UCL original: play 7 times
 2. DCL delivered: play 5 times
 3. UCL updated: play 2 times
- A DCL is protected by encryption with the public key of the device

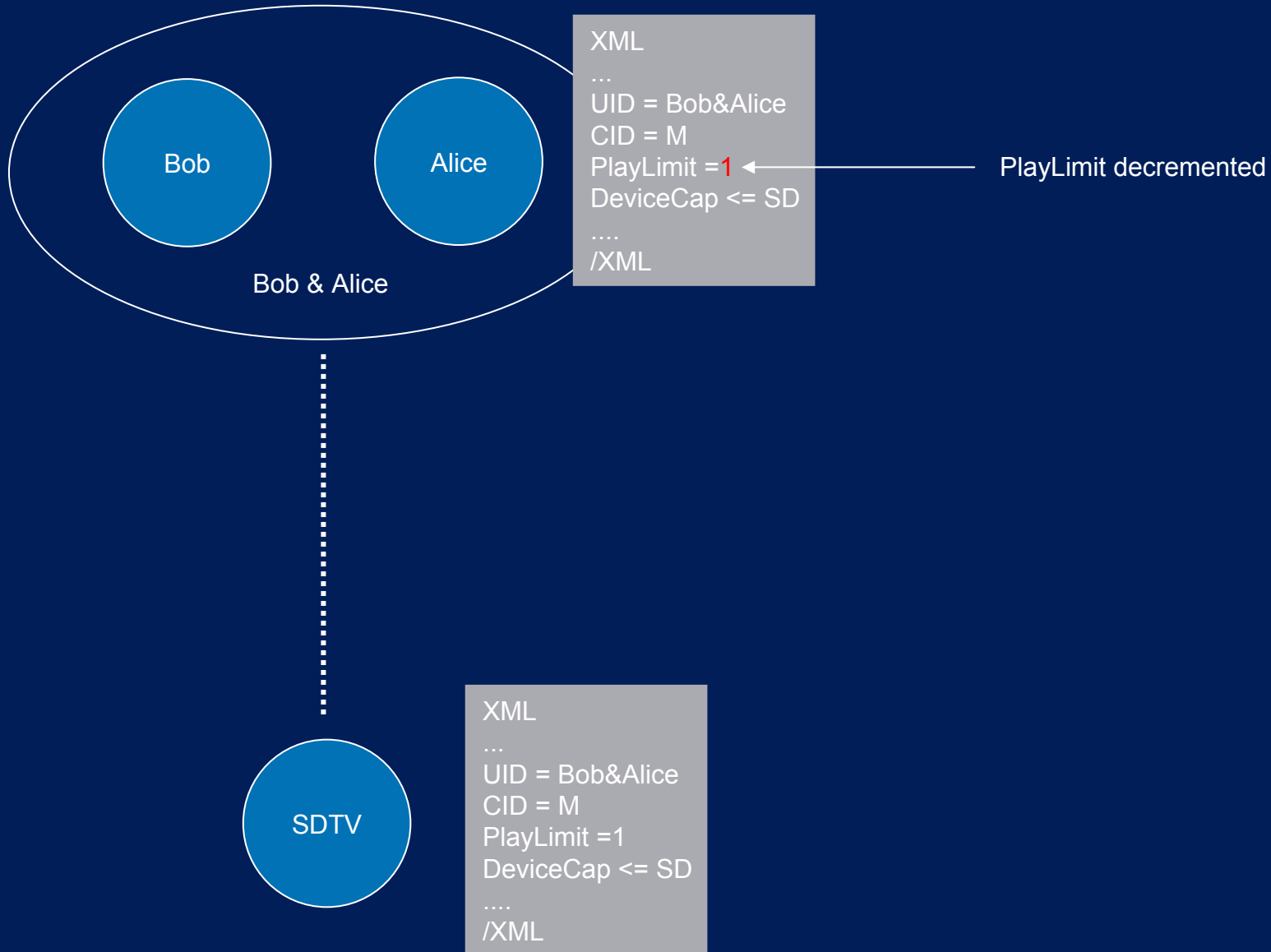
Example – License Acquisition



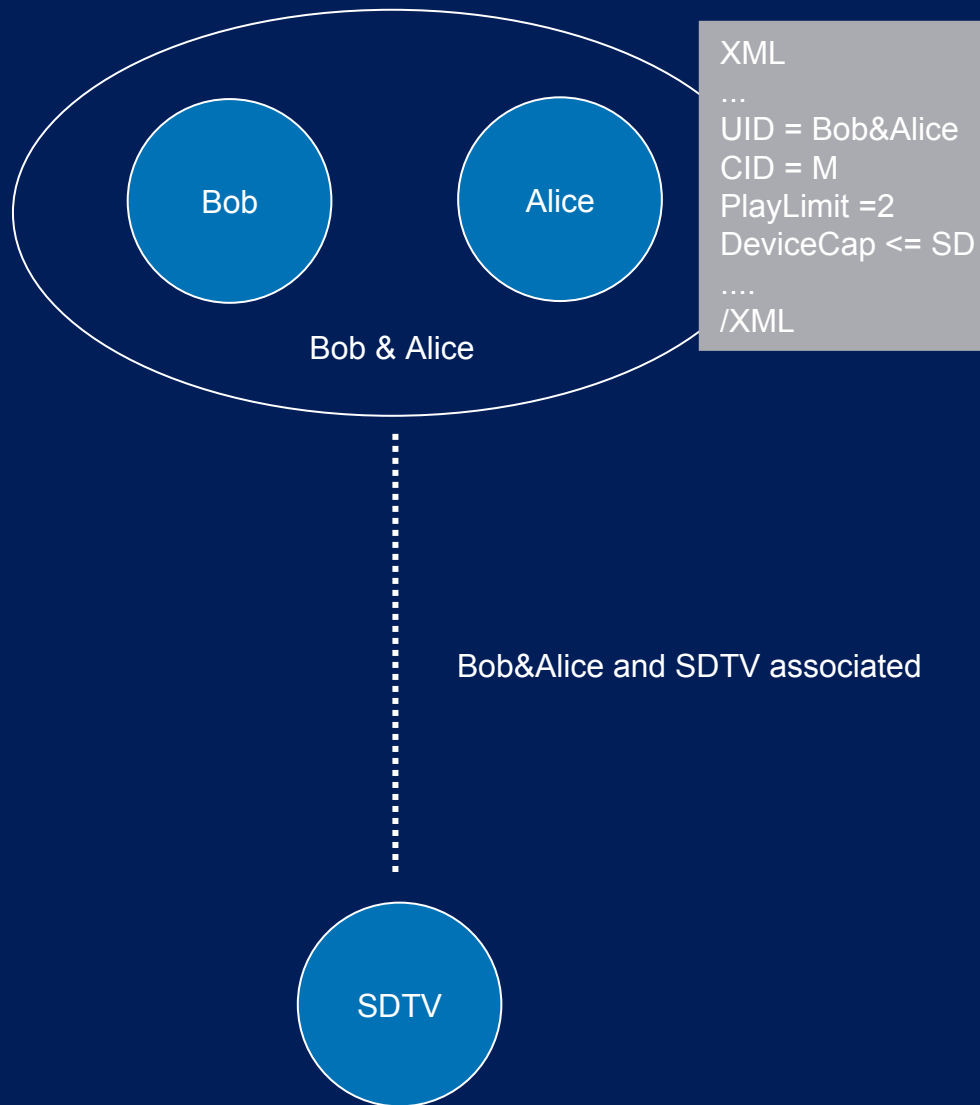
- 2 UIDs – Bob, Alice
- Devices – HDTV, SDTV, Portable TV
- Bob and Alice form User Identity
- Bob&Alice compute (without communicating) their combined private key $K\text{-Priv}_{B\&A}$
- Bob&Alice request movie M, VHS format, to be played twice, from LPr.
- LPr approves and sends license UCL.
- Bob and/or Alice store(s) UCL.



Example – License Delivery to Device



Example – License Delivery to Device



Discussion



- Remaining technical issues
 - Legacy devices that don't have user authentication capabilities
 - Proof of concept built on existing systems (e.g. OMA v 2.0)
- Business models and adoption
 - Establishing universally recognized and trusted identity provider
 - Policies for content distribution to groups of users
 - Transition from existing systems, end user education and adoption

Conclusion



- Limitations of current device centric DRM systems:
 - Enforcement and control of content is associated with a particular device
 - Association between user and content is secondary
 - Limitations on the number of devices that can render content
 - Insufficient flexibility
- Proposed **person-centric DRM system** enables:
 - Access to content **at any time, on any device**
 - Binding of rights to users
 - Devices are anonymous rendering entities
 - Flexibility for distribution of licenses to groups of users