

# On DRM Interoperability and Compatibility

---

Xin Wang  
Chief Scientist  
ContentGuard, Inc.

**Workshop on Digital Rights Management Impact on Consumer Communications, January 6, 2005**, in Consumer Communications and Networking Conference (CCNC '05), January 3-6, 2005, Las Vegas, NV, USA



# Outline

---

- ❑ DRM Interoperability Problem
- ❑ Concepts of Interoperability and Compatibility
- ❑ Confusions
- ❑ Types and Properties
- ❑ Approaches to Interoperability
- ❑ Conclusions

# DRM Systems at Work

---

- Some Existing DRM Systems
  - Microsoft's Windows Media DRM
  - Real Networks' Helix
  - Apple's Fairplay
  - Yahoo's newly acquired MusicMatch
  - OMA DRM
- Some Online Music Ventures
  - Windows Media (Microsoft)
  - Rhapsody (Real Networks)
  - iTunes (Apple)
  - MusicMatch (Yahoo)
  - PressPlay (Napster)

# The DRM Interoperability Problem

---

- Consumers aren't able to use content (e.g., songs) they purchase across different (open or proprietary) DRM systems
  - **Content** created by or for one DRM system cannot be used, distributed and protected by another
  - **Rights** granted by or for one DRM system cannot be honored and enforced by another
  - **Protection** made by or for one DRM system cannot be observed and processed by another
  - **Trust** established by or for one DRM system cannot be embraced and maintained by another
  - **Business models** established by or for one DRM system cannot be adopted and executed by another

# DRM Interoperability Expectations

---

- Consumer
  - any DRM content can be consumed at any time, any place on any DRM device or system
  - choice, flexibility and convenience
- Provider
  - content and rights can be prepared once and distributed by most profitable channels and consumed by any DRM system
  - choice, flexibility and cost effectiveness
- Vendor
  - system components can replace similar components from other vendors
  - market share and cost effectiveness

# Causes for Non-Interoperability

---

- Lack of existence and adoption of open, common standards for
  - packaging and protecting content
  - specifying and interpreting rights
  - establishing and maintaining trust
  - describing and executing business models
- Others include
  - Cost to implement interoperable systems

# Interoperability is now a “Buzzword”

---

- ❑ “End-to-end DRM interoperability”
- ❑ “Content Interoperability”
- ❑ “Device Interoperability”
- ❑ “Rights (Language) Interoperability”
- ❑ “Interoperability in one interconnected system using cell phones, game platforms, PDAs, PCs, web-based content services, discovery services, notification services, and update services.”

# What is Interoperability

---

- ❑ “Ability of a system (as a weapons system) to use the parts or equipment of another system.” Merriam-Webster Online Dictionary
- ❑ “The capability of a computer hardware or software system to communicate and work effectively with another system in the exchange of data, usually a system of a different type, designed and produced by a different vendor.” ODLIS: Online Dictionary for Library and Information Science
- ❑ “The ability of systems or products to work together automatically.” Netlingo
- ❑ “The condition achieved when two or more technical systems can exchange information directly in a way that is satisfactory to the users of the systems.” AAP DRM Report

# Essence of Interoperability

---

- It is about the “ability” of different entities (system/applications/modules) from different vendors to “interoperate” or “work” together
- Consequentially,
  - it is not meaningful for a single entity without referencing others, and to say “an entity is interoperable” (i.e., it has interoperability) must have some additional context about what it is interoperable with
  - it does not apply to a system, all of whose components are from a single vendor
  - it is not an issue if two entities do not need to work together
  - it does not make sense for passive objects, e.g., “a format/language is interoperable”



# Confusion with Exchangeability

---

- “Exchangeability” – Replacing one Entity with another
  - “Can one decryption module (from one vendor) replace another decryption model (from another vendor) to decrypt the same file?”
  - = “Compliance”. Depends on whether it is/is not compliant to whatever the other is compliant with
  - Since exchangeable parts do not need to work together, there is no interoperability issue. Rather, “encryption modules have an interoperability issue with decryption modules”
- Interoperability only exists among interoperating parts!

# Confusion on Intra Interoperability

---

- “Extra” versus “Intra” Interoperability
  - “My system is interoperable with yours”.
    - This is a definitive one.
  - “My system is interoperable” implies “entities in my system work together and they are interoperable”.
    - This is secondary, and conceptually just an abbreviation for convenience.
  
- Interoperability must have its context!

# Confusion with Remedies

---

- “Remedies” – Making non-interoperable entities interoperable
  - “System A understands MPEG REL, and System B OMA REL. Through a translation between the two languages, System A can interoperate with System B.”
  - System A and System B themselves do not have interoperability with each other. Period.
  - With the translation, System A and System B may still not be interoperable, if System C doing the translation is not interoperable (e.g., no standard translation exists between the two languages, and different vendors come up with different translations).
- Remedies themselves must be compliant to standards!

# Interoperability is not Everything

---

## □ There is also **Compatibility**

- The capability of different components from different vendors to be adapted to work together
- Components include
  - Data (passive): MPEG REL is compatible to OMA REL, but not the other way around
  - Applications: Windows Media DRM 10 is compatible with Windows Media DRM 9
  - Devices: iPod Mini is compatible to iPod
  - Standards: MPEG-21 ones to domain ones!

# Why DRM Interoperability is hard to Achieve

---

- Too many things Consumers need to Own and Access
  - Data
    - Content, Rights, Usage information, Identification, Keys, Certificates
  - Devices
    - Hardware modules, Gadgets
  - Applications
    - Software modules, Services
- Too many things DRM systems need to take care of
  - Identification and Declaration (metadata)
    - Content, users and devices
  - Rights
    - Rights expressions, rights data, and exercise states
  - Protection
    - Encryption, signatures, watermarks
  - Key management
    - Key hierarchy for encryption and signing
  - Trust management
    - Trust root, hierarchy, policy and establishment

# Understanding Interoperability

---

## Primitive Interoperations

	<b>Direct</b>	<b>Indirect</b>
<b>Loose</b>	<b>Protocol</b> (e.g., Web server and client)	<b>Data/Messages</b> (e.g., video encoder & decoder)
<b>Tight</b>	<b>Interface</b> (e.g., plug-in modules)	<b>Bridging Interface</b> (e.g., power plug adapters)

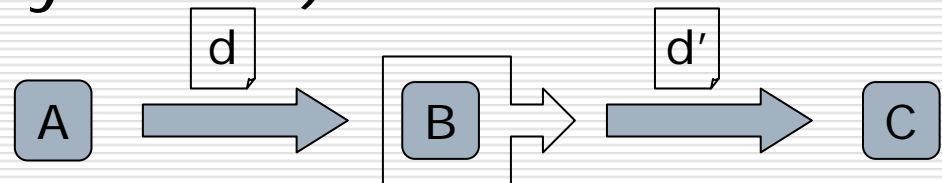
Categorization based on Coupling and Interaction

# Understanding Interoperability

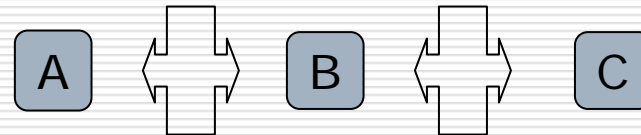
- Composite Interoperations

- Basic (3rd party based)

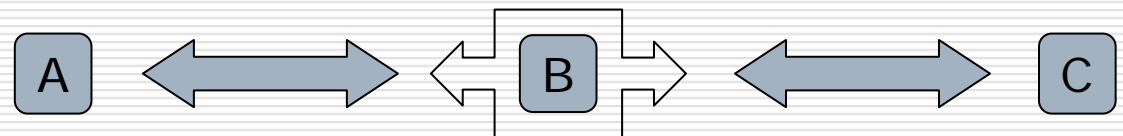
- Data mapping



- Interface adaptation



- Protocol translation



- Hybrid (repeat and combine above)

# Types of Interoperability

---

## □ Data-based

- Can B exercise rights issued by A?
- If B understands the rights language A uses

## □ Interface-based

- Can B react to A's call to decrypt content?
- If B exposes an interface that A can call

## □ Protocol-based

- Can B interact with A to acquire a license?
- If B and A follow the same protocol for license acquisition

# Properties of Interoperability

---

## □ "Symmetry"

- $A \Leftrightarrow B$  if and only if  $B \Leftrightarrow A$
- This is different from that A and B may have asymmetric roles (one as server and the other as client)

## □ "Non-Transitivity"

- $A \Leftrightarrow B$  and  $B \Leftrightarrow C$  MAY NOT imply  $A \Leftrightarrow C$
- A and C speak two different languages, both of which B understands

## □ "Composeability"

- $A \Leftrightarrow B$  and  $B \Leftrightarrow C$  MAY result in  $A \Leftrightarrow C$  with B's help
- B speaks two languages and acts as the translator

# Properties of Compatibility

---

## □ "Asymmetry"

- $A \rightarrow B$  does not necessarily imply  $B \rightarrow A$
- Different from symmetry of interoperability

## □ "Transitivity"

- $A \rightarrow B$  and  $B \rightarrow C$  imply  $A \rightarrow C$

## □ "Composeability"

- $A \rightarrow B$  by  $X$  and  $B \rightarrow C$  by  $Y$  imply  $A \rightarrow C$  by composing  $X$  and  $Y$

# Relationship between Interoperability and Compatibility

---

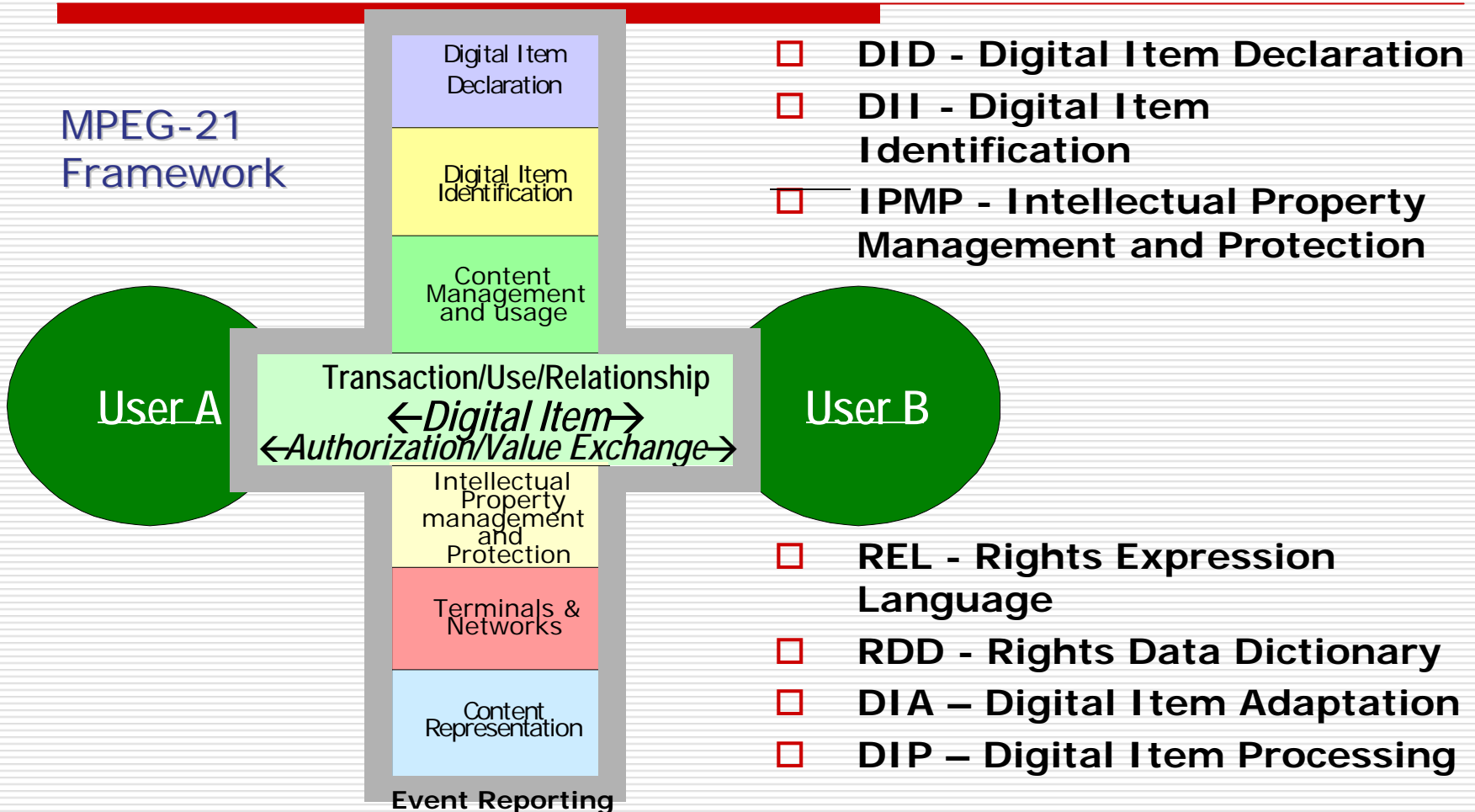
- Compatibility is implied by Interoperability
  - No adaptation is needed if interoperable
  - But the reverse is not true
- Non-compatibility implies non-interoperability
- Interoperability may be achieved through Compatibility
  - If the adaptation is also interoperable with the compatible parts

# Approaches to Interoperability

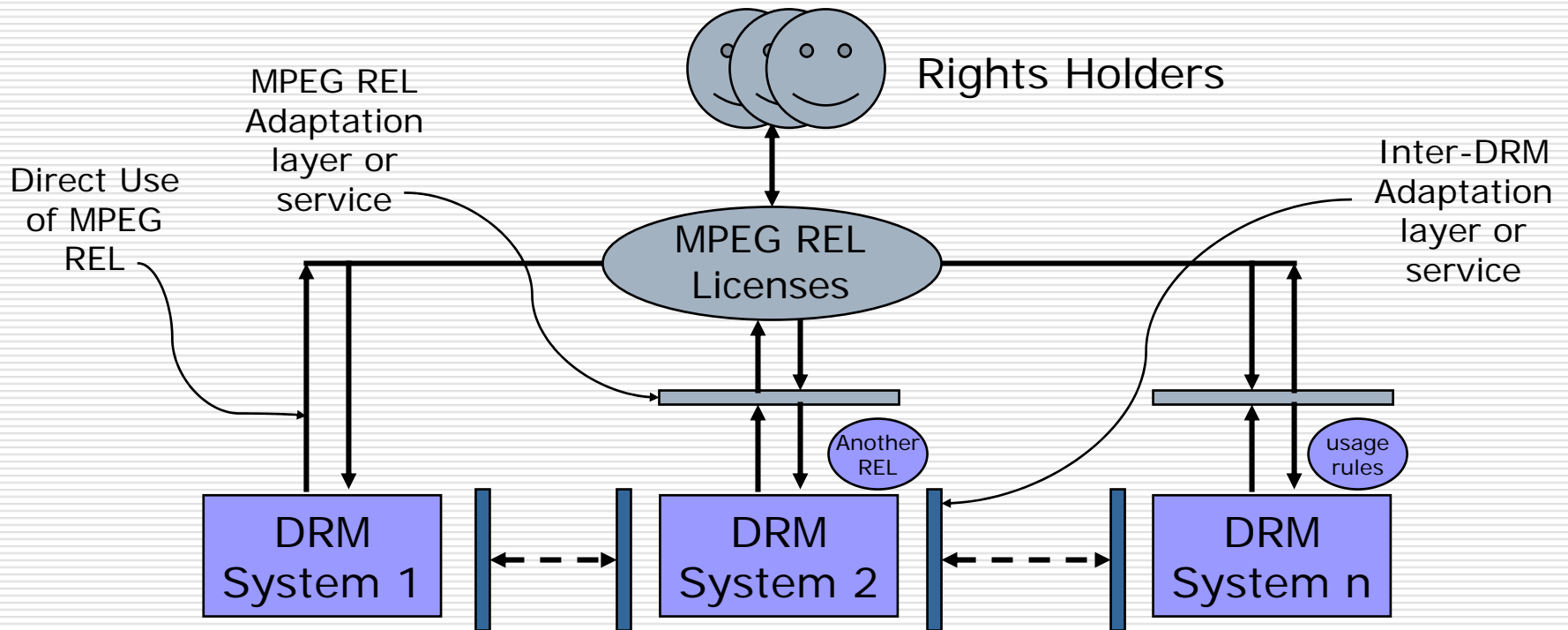
---

- Principle – “Interoperability is only possible when the systems or products conform to standards.” Netlingo
  - Standards can be industry led or de-facto but need to be open
- From scratch
  - Standard Data Format
  - Standard Interface
  - Standard Protocol
- From non-interoperable legacy entities
  - Share standard exchangeable data format
  - Introduce standard adaptive interfaces
  - Connect standard intermediate protocols
- Through non-technical means
  - Drive some non-interoperable entities out of market
  - Reduce alternative, non-compatible standards

# Interoperability from Scratch



# Interoperability by REL



————→ required  
- - - - -> optional

# Not Every “Standard” Supports Interoperability

---

- ❑ Not sharing state information about content usage
  - Count (e.g., 5 times)
  - Metered and floating time intervals (e.g., 5 metered hours, and 5 floating, continuous days)
- ❑ Simply specifying rights without indicating how to share state information does not ensure interoperability
  - After one player plays 3 times, how does another player know that it can only play 2 more times?



# Non-interoperability Issue with the "Broker" or "Service" Approach

---

- ❑ System A's interface may be converted into System B's interface, by use of a "broker" or "service" C, and A and B may work together via C
- ❑ But the big system including A, B and C may still not be interoperable if C is not
- ❑ In order to make the entire system interoperable, the "broker" or "service" C must also conform to standards.

# A Compatibility Perspective on DRM Interoperability

---

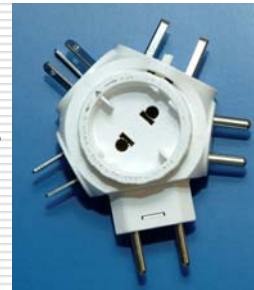
□ An ideal situation is



□ But, the reality is



□ However, there are



# Conclusions

---

- ❑ Interoperability is about interoperating entities from different vendors
- ❑ It can be achieved from non-interoperable, compatible entities, but extra integrating entities must also be interoperable themselves by being compliant to open standards
- ❑ Interoperability can be achieved only by standards
  - Open standards enable interoperability
  - Monopolies or authorities drive interoperability away
  - Anything in between leads to heterogeneity
- ❑ Interoperability is great to have, but needs to be balanced with effectiveness and efficiency.
  - Life would be much easier if there were less alternatives that need to be interoperable!
  - If people cannot agree on a single standard to interoperate, then at least need to make all the standards compatible!

# Thank You

---

[xin.wang@contentguard.com](mailto:xin.wang@contentguard.com)

[www.contentguard.com](http://www.contentguard.com)