Security and DRM

Joseph Chou
Texas Instruments

Security and DRM

- DRM is Based on Security Principals
  - Authentication (device, user, service)
  - Key management, data encryption and signature for data confidentiality and integrity
  - Secured delivery of premium content usage rights
  - Can be used for personal content protection
- DRM Interoperability is Needed
- PERM Interoperability Framework

Issues with DRM System Diversity

- Lack of a unified and open DRM system standard for PC, CE and mobile handheld devices for broadcast, internet and packaged content interoperability
- Current DRM system implementations are not interoperable
  - Diversity of smart card/CI implementations
  - Diversity of internet DRM system implementations
  - Diversity of packaged media content protection implementations
- Mismatches between different trust and protection models
- Mismatches between rights expression languages
- Consumer devices cannot locate and connect to all needed services/content

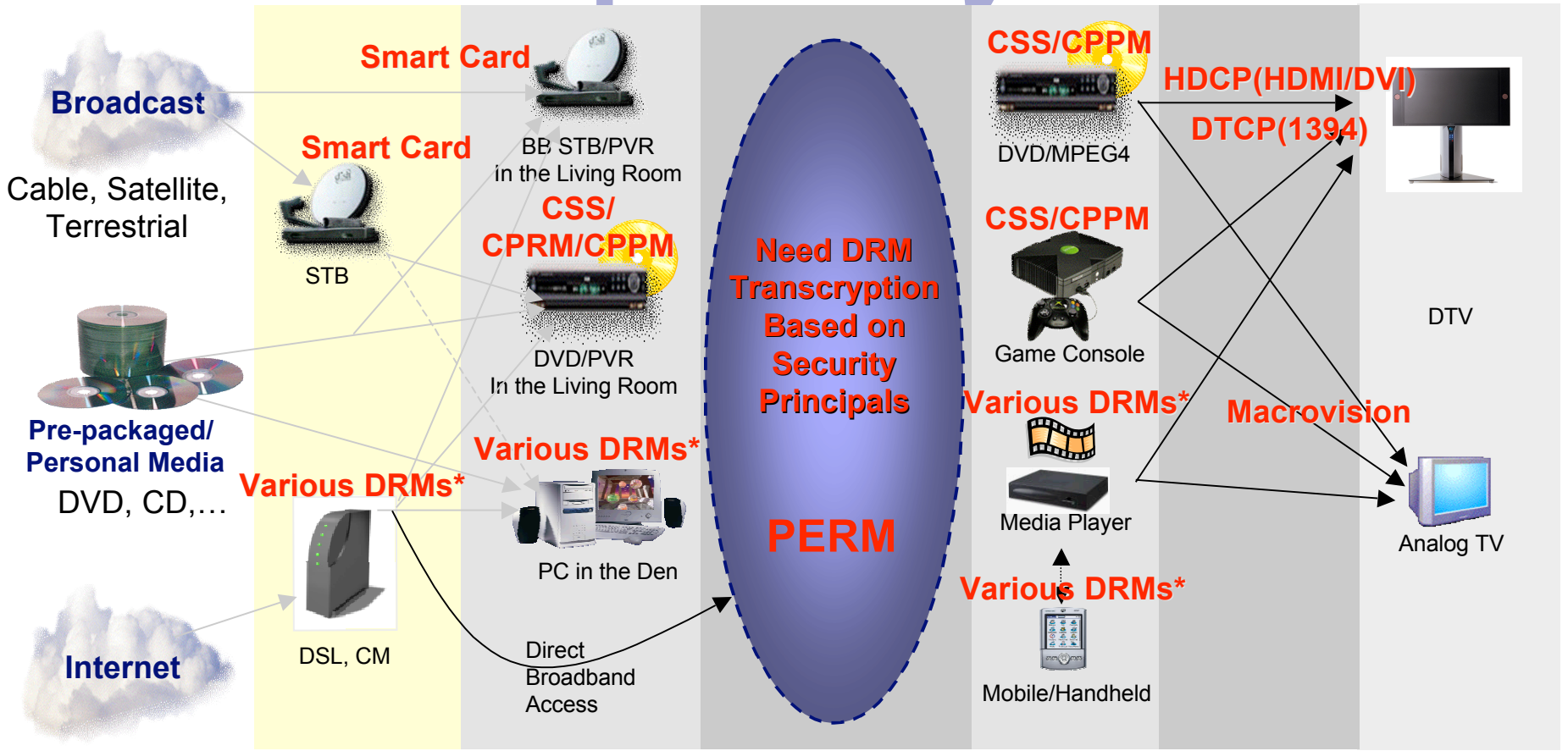
Diversity of Security, Content Protection/DRM Implementations

- Pre-recorded/Recordable content (DVD, DVD-Audio)
  - **CSS** (Prerecorded DVD)
  - **CPPM** (Prerecorded Audio)
  - **CPRM** (Recordable Audio/Video)
- Internet streaming audio/video content
  - **Various DRMs**
    - WM DRM 10, Fairplay, Real, Open Magic Gate, OMA, SDMI and etc.
- Broadcast content
  - **Smart Card DRMs**
    - DigiCipher, Cable Card ITU-T SG9, DVB-CSA, DirectTV, Multi-2, NDS (ICAM), Irdeto, Nagra, DVB Content Protection and Copy Management (CPCM) and many others.
- Between media client and TV/display
  - **HDCP** (HDMI/DVI)
  - **DTCP/1394/USB** (1394/USB)
  - **Macrovision** (analog TV)

Rationales of DRM Interoperability Framework

- Users are able to locate and connect to the content services that they need
- A security protocol can be used to protect personal contents or clear contents from the original content owners
- An open DRM interoperability standard accelerates content consumption in the home network and propels device volume growth and thus benefits the consumers, the content owners and the device manufacturers

DRM Interoperability



Source	Access	Media Server	HNET Bridge	Client	AV Cable	A/V Device

Authentication
Encryption
Integrity