DRM
Digital Rights Management

October 29th, Cologno Monzese

CONTEXT

Digital technology:

- made it easier to copy and share content illegally;
- but also enabled new business models that benefit both content producers and broadcasters.

Thanks to DRM systems, it's possible to manage both content protection and business models effectively.

DRM is central to all content licensing agreements with third parties — defining both **commercial** use and **protection** rules.

MEDIASET

GENERAL DISPOSITIONS

A typical deal with a major – covering Free Tv, Catch-up TV and SVOD – usually includes the following **requirements**:

Licensed content **when distributed via the open internet** must be **transmitted and stored with encryption**, under a **DRM system** approved by the licensor.

Dedicated license acquisition for each approved device.

Each **device must be indentified** before it can access the license.

MEDIASET

DEVICES

Contracts include a **detailed list of authorized devices** and define:

- Operating **conditions** for **each category** (Smart Tvs, STBs, PCs, dongles…).
- Devices **denied access** to licensed content.

Connected CE devices may include:

Closed-access equipment operating via Internet connectivity, such as:

- *Digital media receivers (e.g. Roku, Amazon Fire Tv)*
- *Blu-ray players*
- *Video game consoles (e.g. Xbox, Playstation)*
- *Intenet-connected TVs*

Excluded devices:

Any consumer electronics **not properly curated or maintained** to ensure:

- *Content integrity*
- *Security compliance*
- *Copyright protection*

LICENSE AND DEVICES

Every license shall:

- Be **cryptographically linked** to a **single approved device**, preventing use or migration to others unless explicity allowed;
- Include measures to **prevent re-encoding or retransmission** of the stream by PCs or mobile devices;
- **Restrict forwarding or mirroring** the stream (as tabcasting) to specific allowed devices (e.g. Chromecast, Google Cast, or other HDMI-connected receivers) to protect licensed content.

SECURITY

The approved **content protection system** and all **authorized devices** **must exclude**:

- **Control mechanisms** capable of altering protection functionality;
- **Debug interfaces** or diagnostic tools;
- **Software implementations** that could compromise protection systems exposing **decrypted content** to unauthorized access, duplication or distribution.

CONCLUSION

Managing Content Protection across devices is essential for content distribution over the Internet:

- Identifies the **device** requesting the content
- Checks **DRM type and compliance**
- **Blocks delivery** if requirements aren't met

This obviously applies also to Open Environments (HbbTV)

DRM =
Security + Compliance + Business continuity

That's why **DRM are essentials for the industry**

MEDIASET