Anti-counterfeiting and anti-piracy technology guide

https://euipo.europa.eu/anti-counterfeiting-and-anti-piracy-technology-guide

Digital Rights Management (DRM) Systems

DRM systems control who accesses and uses digital content. Most people have probably come across one, perhaps without even realising it, thanks to the growing popularity of online streaming and gaming. When streaming platforms limit the number of devices per account, or when games companies require users to input a product key before playing, that is a DRM system at work, protecting the digital copyrighted content.

Used for	Goes on	Can be used for
Authentication	Product	Digital products
Tracking/Tracing		
Anti-tampering / Anti-alteration		

Visibility	Reading device needed	Connection to server
Invisible	Yes	Yes

Description

DRM systems are designed to combat the large-scale, unauthorised copying and distribution of digital copyrighted content that takes place via the internet. They use two core processes to help copyright and associated rights holders protect and control access to their digital property:

- inclusion of metadata: data (such as the purchaser's name or account information) that can only be read by specific software are embedded in the digital files;
- encryption: the digital content is written in a code legible only by devices or software that have an encryption key, which is made available offline or online depending on the authentication procedures.

By encoding and encrypting digital files, DRM systems make these files very difficult to duplicate (outside of the managed environment) and ensure that their use is limited (to certain periods of time or specific uses) and subject to the terms of the access licence granted to end users.

Uses

DRM systems target the counterfeiting of digital content such as audio and video files, e-books, software and computer games. They are mainly used to:

- certify the lawful use of digital files and/or full ownership of copyrighted content, making it possible to distinguish authorised copies from pirated copies (authentication);
- ensure legitimate access to content by embedding special digital markers in the original file or by distributing the file in a protected format;
- control pirated copies by making it possible to track the initial holder of the original files (tracking);
- control payment for the services.

Implementation

If you want to use a DRM system, you will need to put processes in place to make sure that, during production,

the metadata is generated and embedded in the digital file, and/or that its content is encrypted.

Cost

The costs associated with DRM systems are highly context-specific, making it difficult to give a general idea of the resources required.

*The information contained in this site is of **general** informational nature and does not constitute legal, consulting or any other **professional advice or guidance**. The information contained in this site is provided on an 'as is' basis with **no guarantee of completeness**, accuracy, usefulness or timeliness and without any **warranties** of any kind whatsoever, express or implied, including but not limited to warranties of performance, merchantability and fitness for a particular purpose. The use of the information is at the user's own risk and the EUIPO does **not guarantee any specific results** or outcomes based on the use of the information provided on this website. The search results are **not presented in any order of recommendation** . This website contains links to **other third-party websites**. Such links, which are free and publicly available, are only for the convenience of the user or browser; the EUIPO does **not recommend, endorse**, warrant, or assume liability of the content or practices of these third-party sites. The EUIPO may update, modify, or remove any information on this website without prior notice. It is the user's responsibility to stay informed of any changes.*