Datasheet


# Irdeto Tracemark™ for OTT head-end

## Forensic watermarking to protect live and on-demand content delivered over-the-top (OTT)

Video viewing habits have changed across the world, especially among younger consumers. People increasingly watch movies, TV series and sports on personal devices via an OTT service – sometimes even exclusively – due to attractive content offerings, pricing and convenience. Unfortunately, pirating OTT content and illegally redistributing it over the internet has also become easier with the wider availability of technology and increased broadband speeds. Internet redistribution piracy is now the greatest threat to the media business. The accelerated move to OTT can also be attributed to the coronavirus pandemic.

If you want to offer a competitive OTT service that will increase both revenue and profit, you must have a security strategy that enables you to acquire premium content and protect its value from piracy. Content owners such as Hollywood studios and sports rights holders have increased the security requirements for premium content in order to combat content redistribution piracy. With the introduction of ultra-HD (UHD) content, multiple studios have defined a set of security requirements which all providers must meet in order to be eligible for premium content such as early release movies. These include forensic watermarking and breach/piracy response to help service providers stay one step ahead of the pirates.

Irdeto TraceMark for OTT is a forensic watermarking solution that embeds a unique, persistent, and invisible mark to identify both the content and individual streams. It protects video on demand (VOD) and live content such as sports, delivered over the Internet. When used in conjunction with Irdeto Cyber Services and/or Online Piracy Detection (OPD) services, it provides a quick and easy method to trace the content or stream back to the source of the leak and enable service providers to take actions against the pirate(s). TraceMark is also pre-integrated with Irdeto Control, the multi-DRM and policy management system to help you launch OTT services that support the widest range of devices and business models.

# KEY BENEFITS

### Renewable, robust security to meet stringent requirements

The central architecture is inherently secure. It makes it almost impossible for pirates to tamper with the watermark on the client device. However, it is easy to renew security from the headend if a breach occurs. Content is watermarked as part of the operator's content preparation workflow before being released from the operator's secure premises to the CDN.

TraceMark for OTT inserts a robust, high-fidelity watermark that is invisible to viewers and compliant with Hollywood studio requirements. This ensures viewers enjoy the best picture quality possible while enabling the best protection of premium content. The solution is capable of consistently identifying the offender's session even when content is redistributed in different formats and/or manipulated using video compression, cropping, luminance filtering, blurring or scaling techniques.

### Ease of deployment and scaling

TraceMark for OTT embeds forensic watermarking at the headend. This means consumers can receive and view watermarked content on any device, without requiring any changes to their client-side hardware or software.

TraceMark for OTT is also DRM agnostic. The operator can encrypt watermarked content on its headend using any of the common DRM technologies available today. Furthermore, the DRM client in the consumer device is completely unaffected by the watermarking. The solution is pre-integrated with many popular encoders and CDNs, as well as Irdeto Control for multi-DRM and policy management. This level of end-to-end integration makes it quick and easy to deploy forensic watermarking to your ever-increasing consumer base and wide range of devices.

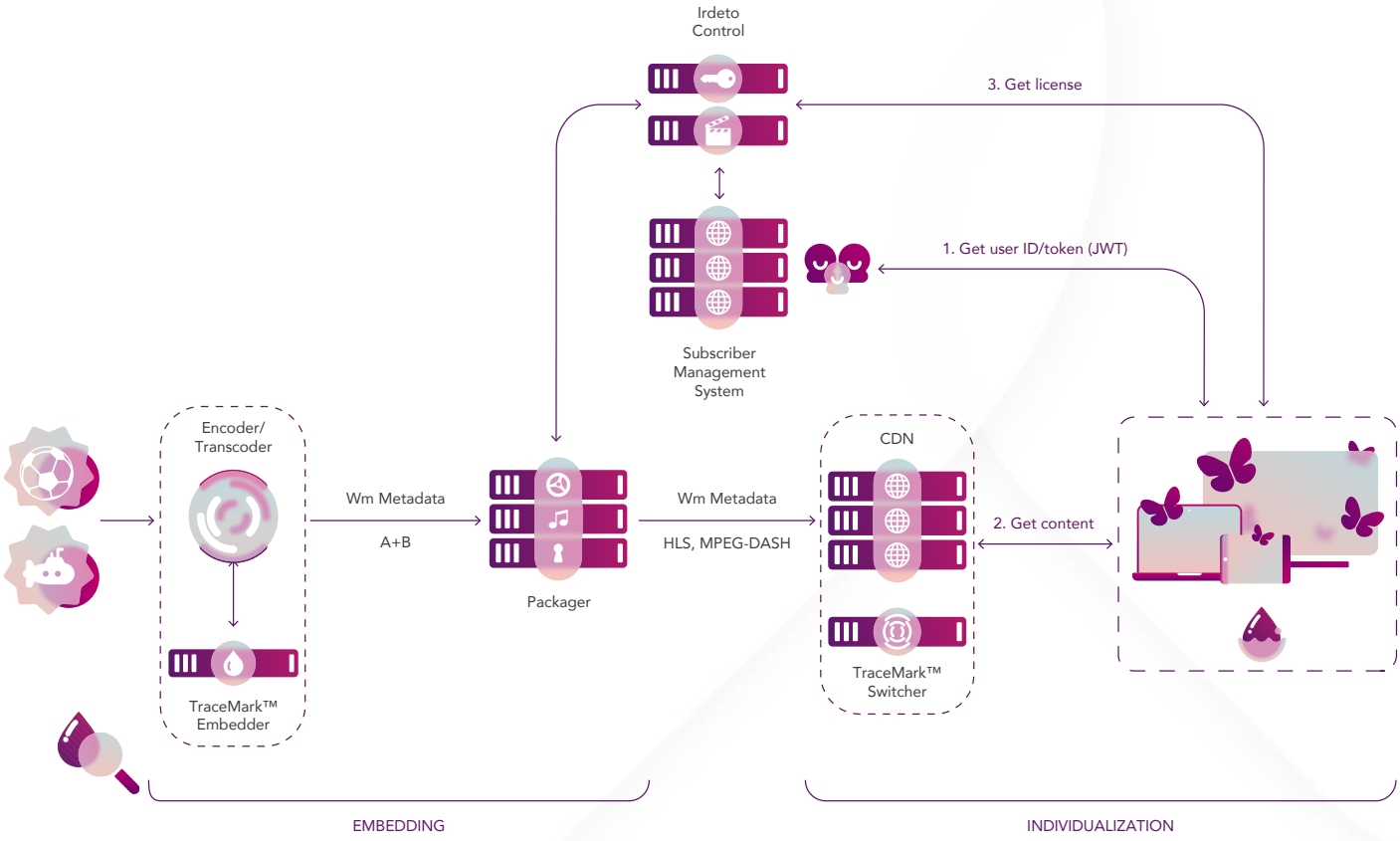
### Effective defense against content redistribution piracy

Having state-of-the-art watermarking technology on its own does not provide the maximum benefits. The winning formula involves robust and scalable forensic marking technologies combined with proactive enforcement and investigative services. With TraceMark, service providers can easily and quickly identify the source of the leak using session-based watermarking. Irdeto Cyber Services and/or Online Piracy Detection services then enable service providers to find leaked content on the internet and identify the source of the leak using TraceMark. By providing actionable insights Irdeto helps service providers shut down rights-infringing services and prosecute parties involved in the piracy.

# HOW IT WORKS

TraceMark for OTT provides encoder-integrated watermarking for VOD and live content on IP networks using HTTP adaptive bitrate streaming protocols such as HLS and MPEG-DASH.

This headend-based approach to session-based watermarking ensures that each device receives a uniquely watermarked version of the content and consists of two steps:




*Encoder Plugin deployment – Preferred Architecture*

- Pre-processing: In this stage, two copies of each video segment are encoded and a different watermark is inserted into each copy to form A and B versions of the video segment. The software component that performs this function can be hosted on-premise or in the cloud:
    - Irdeto TraceMark Embedder inserts watermarks into content video streams during the encoding process, minimizing any delay in the content delivery process or disruption to the content preparation and delivery workflow.

- Post-processing: In this stage, the watermarked copies are interleaved into unique sequences of video segments such that each viewer receives a version of the content like no other (for example, AAAAA, BBBBB, ABABA). This uniqueness is what enables Online Piracy Detection services to pinpoint the content leak to a specific session or user ID. The unique sequence creation function can be integrated within the CDN or hosted on- premise or in the cloud:

    - Irdeto TraceMark Switcher dynamically creates individualized patterns to form millions of unique sessions. Client applications are required to supply session tokens to the CDN. The verification and the interleaving of the segments to create and deliver individualized streams to the users are performed at the CDN edge nodes (Edge Switching). This scalability ensures content protection across a massive viewer base for any service provider.

- TraceMark for OTT can work independently from DRM and is DRM agnostic. And there is no need for client changes or client processing, as the content arrives already watermarked in the regular content format. This means there is minimal impact on the consumer, and both managed and unmanaged devices are covered. By using tools such as TraceMark for OTT, we can all be prepared for the turbulent tides of new vulnerabilities and piracy threats.

Cartesian is trusted and recommended by the major Hollywood studios. Its auditing services comply to the studios rigorous standards, including MovieLabs Enhanced Content Protection specification for Ultra HD and 4K content. The Farncombe Security Audit® Watermark provides confidence in the robustness of the watermark technology tested.


Irdeto is the world leader in digital platform cybersecurity, empowering businesses to innovate for a secure, connected future. Building on over 50 years of expertise in security, Irdeto's services and solutions protect revenue, enable growth and fight cybercrime in video entertainment, video games, and connected industries including transport, health and infrastructure. With teams around the world, Irdeto's greatest asset is its people and diversity is celebrated through an inclusive workplace, where everyone has an equal opportunity to drive innovation and support Irdeto's success. Irdeto is the preferred security partner to empower a secure world where people can connect with confidence.

Last modification: 26-10-2022 / 02:55 pm GMT+01:00