Protect. Renew. Empower.

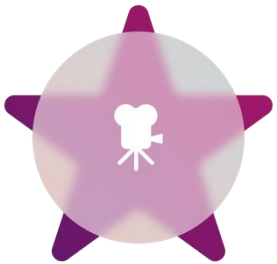
Dutch Guild 59 – Content Piracy Forensic Watermarking

November 2024

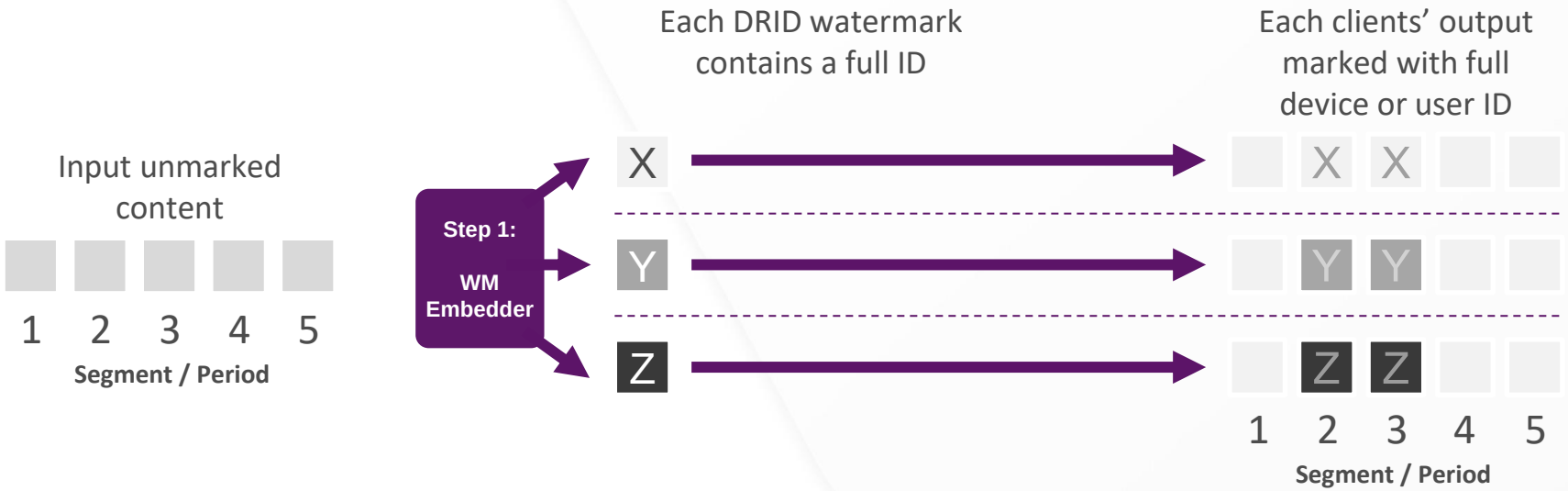
Ronald Peters

Why Forensic Watermarking

- Targeted at high-value (live) TV & movie content with support for 4K UHD
- Content owner compliance (MovieLabs, Premium Live Sports, VoD License owners)
- Identification of illegally distributed assets, reactive tool with deterrent effects
- Can be applied at B2B (distribution) or B2C level



Every receiver a unique copy

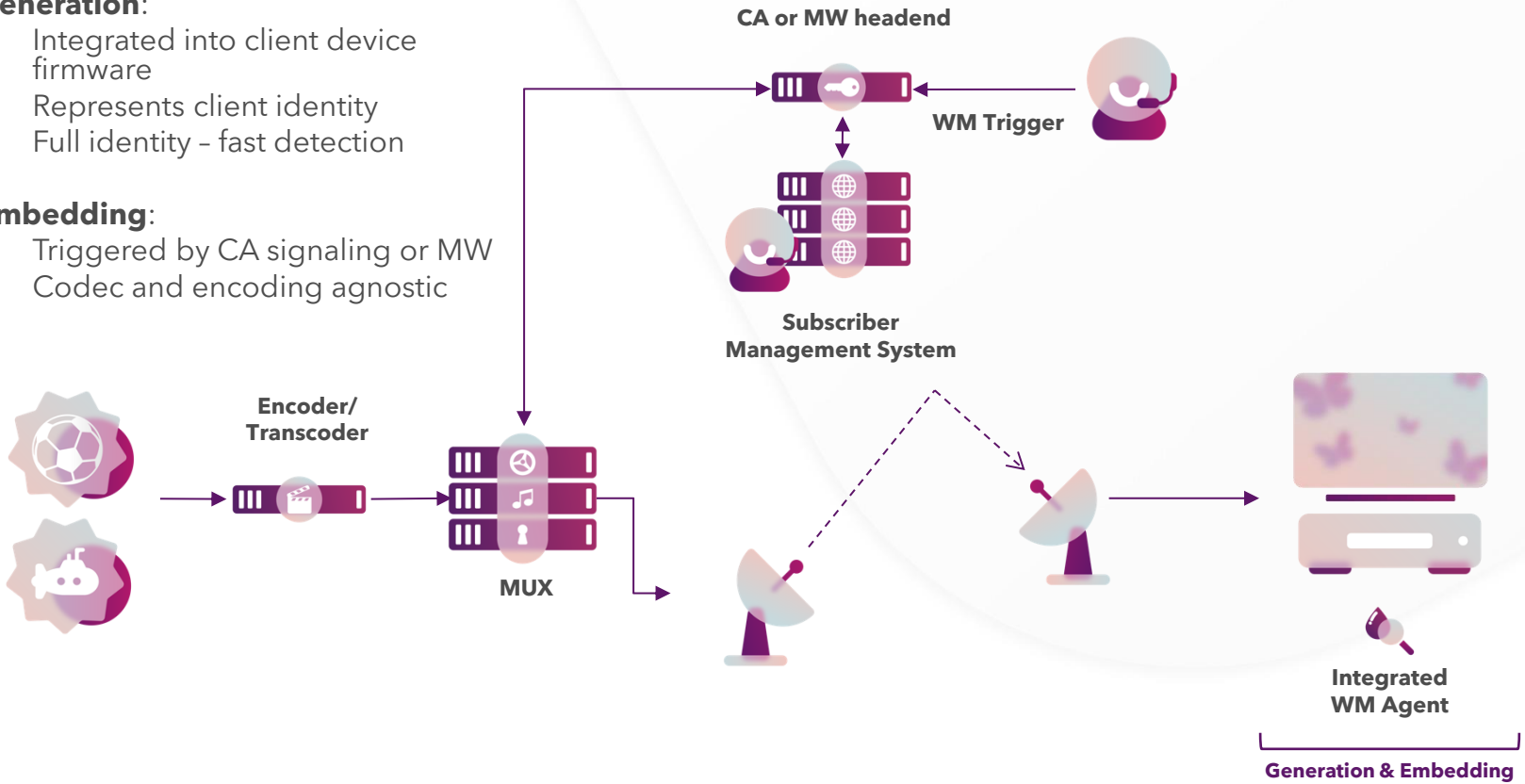


- In use for short clips (DWM/Headend), Broadcast Client, OTT Client
- Embedded in multiple frames
- Detected from a single frame

Broadcast Client-Side Watermarking

Generation:
- Integrated into client device firmware
- Represents client identity
- Full identity – fast detection

Embedding:
- Triggered by CA signaling or MW
- Codec and encoding agnostic

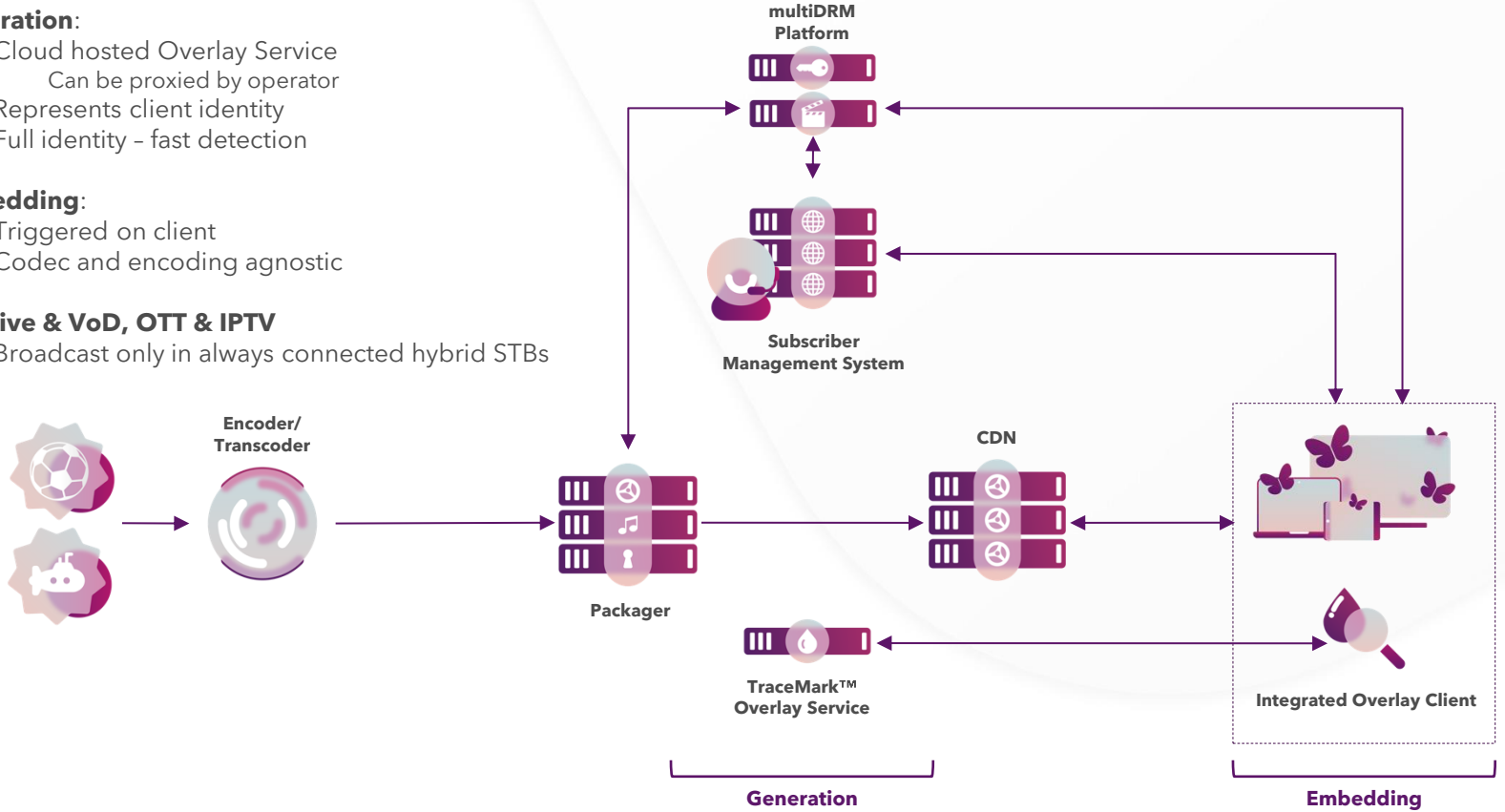


OTT Client-Side Watermarking

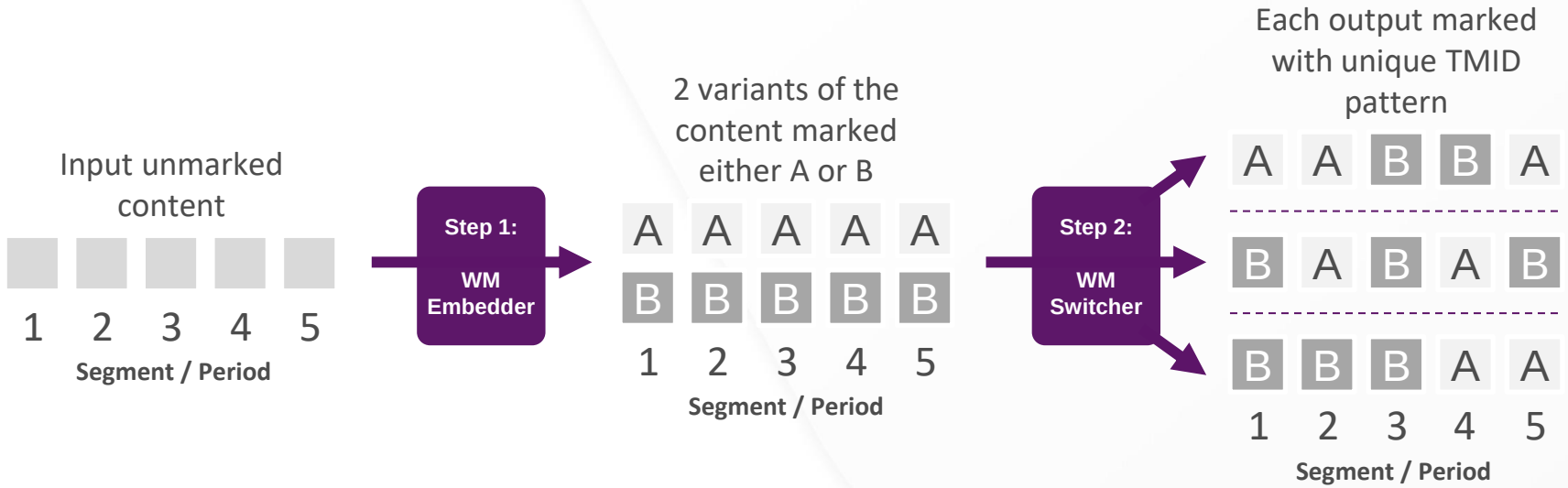
Generation:
- Cloud hosted Overlay Service
  - Can be proxied by operator
- Represents client identity
- Full identity – fast detection

Embedding:
- Triggered on client
- Codec and encoding agnostic

Fits Live & VoD, OTT & IPTV
- Broadcast only in always connected hybrid STBs



Every receiver a unique copy, over time



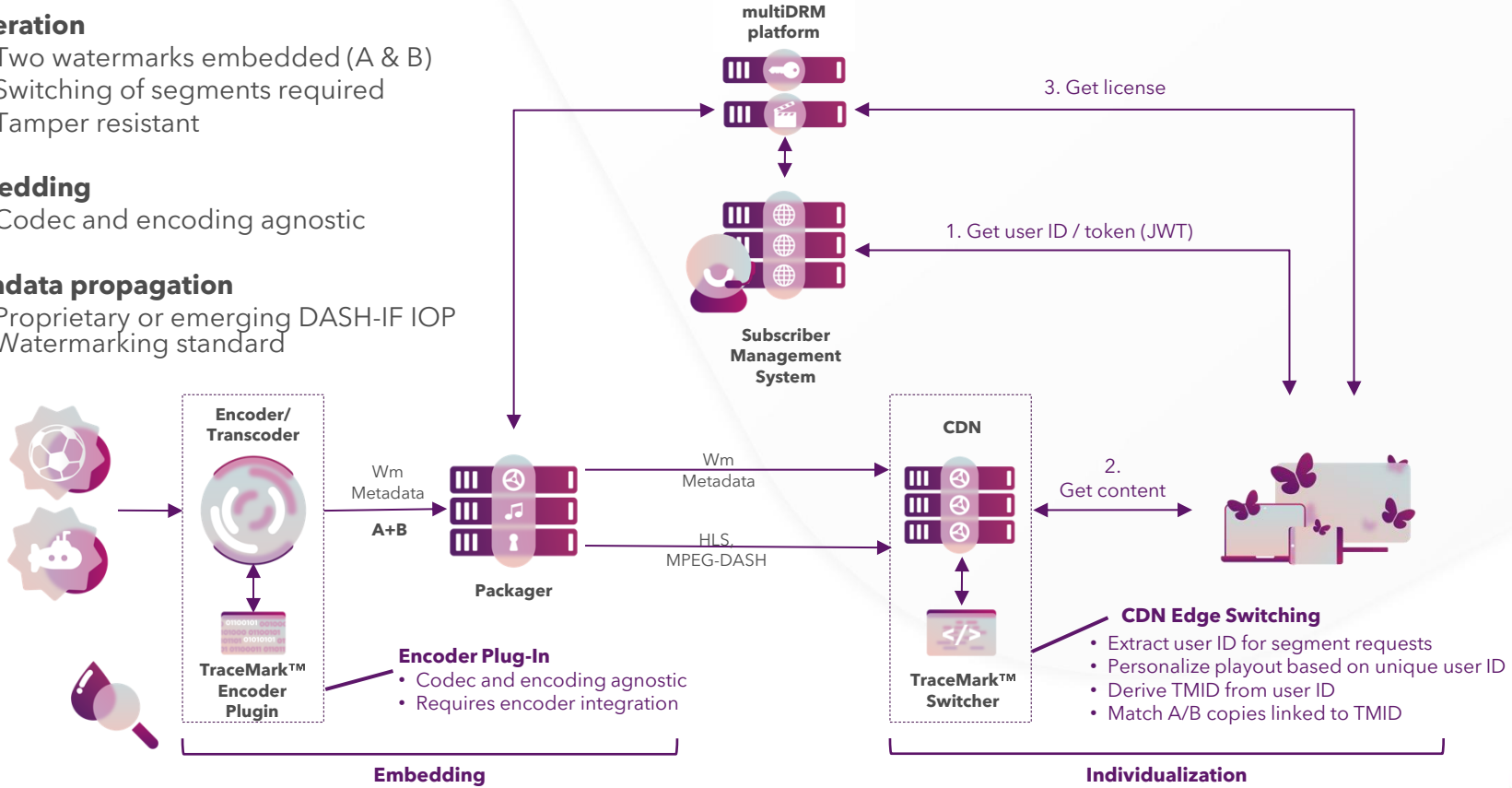
- Used to reach many users from only two segment copies (A/B)
- In use for longer clips (>10 minutes) DWM/Headend

B2C A/B watermarking for OTT Server-Side

Generation
- Two watermarks embedded (A & B)
- Switching of segments required
- Tamper resistant

Embedding
- Codec and encoding agnostic

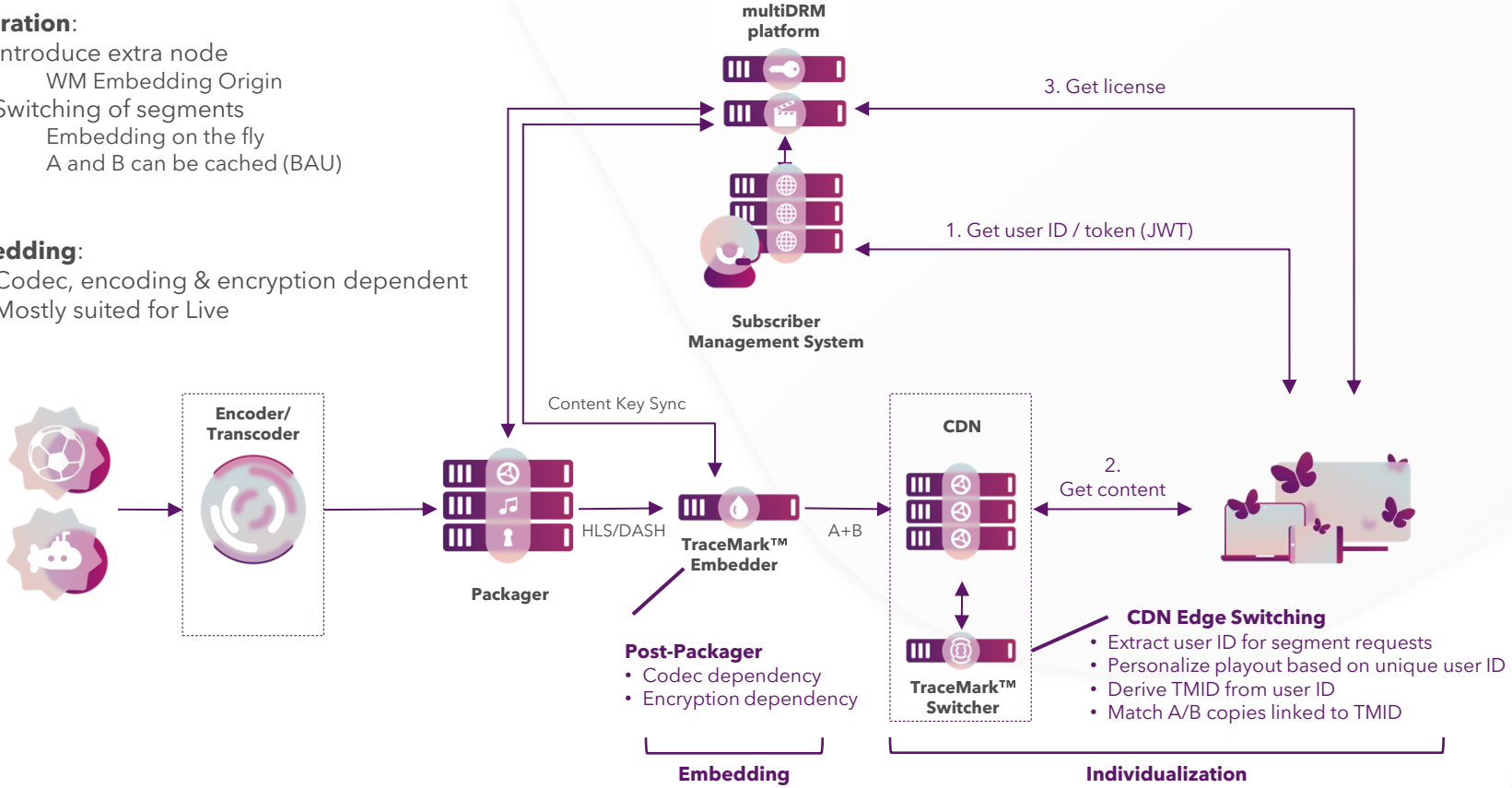
Metadata propagation
- Proprietary or emerging DASH-IF IOP Watermarking standard



What if you can't get into the encoder/transcoder?

Generation:
- Introduce extra node
  - WM Embedding Origin
- Switching of segments
  - Embedding on the fly
  - A and B can be cached (BAU)

Embedding:
- Codec, encoding & encryption dependent
- Mostly suited for Live

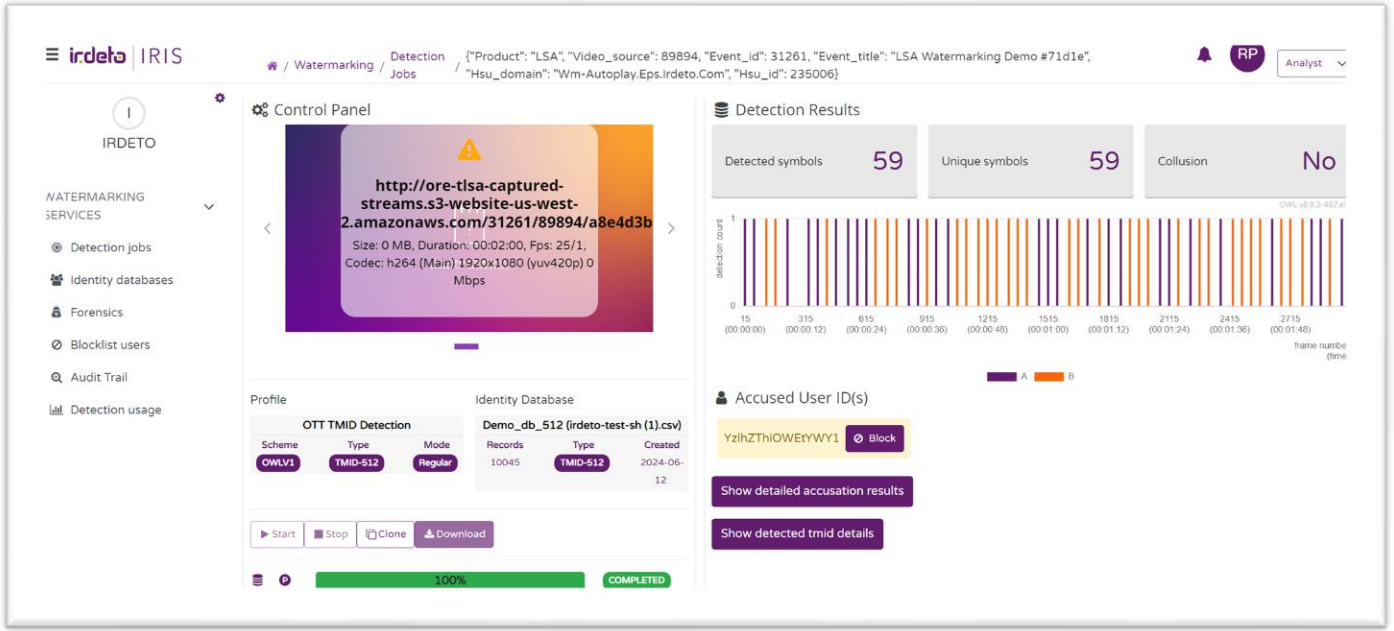


OTT: Head-End vs Client-Side Watermarking

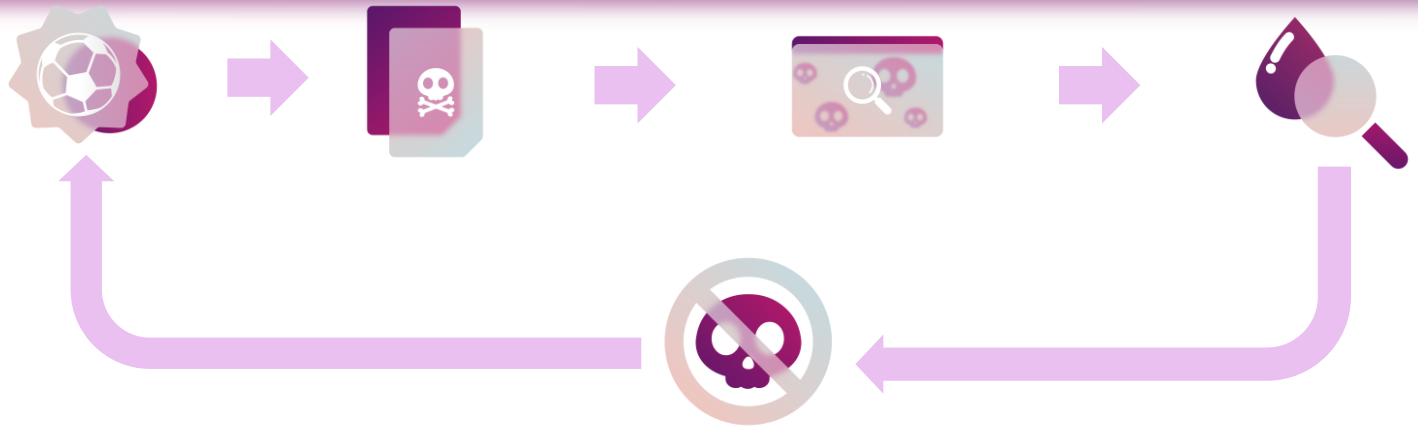
Head-End Watermarking	Client-Side Watermarking
Reach both managed and unmanaged devices	Generally, only for closed, managed devices
Less prone to reverse engineering	Vulnerable to circumvention attacks
Less visible to end-users	More visible to end-users
Requires more video to identify the watermarking identity	*Less video required for watermarking detection*
Upgrades to the watermark easy to perform centrally for all devices	Difficult and costly to upgrade and maintain, especially as device type base diversifies over time
Additional infrastructure required for additional content and channels	*Available for all content streamed by the platform*
Strong against collusion attacks	Weaker against collusion attacks
Compliant to all content owners	Compliant to some content owners
Best architecture to catch pirates	Less suitable for catching (today's) pirates

TraceMark™ Watermark Detection Service

- AWS based managed service, accessible by GUI and API's
- (Blind) Detection from files and live feeds, returns detected id from the CDN token
- Needs minimum of 1 minute video for A/B WMing, 5-10 recommended, longer in case of collusion
- Optional integration with CDN revocation services (blocklist)



Demo Introduction



irdeto

Protect. Renew. Empower.