Forensic Watermarking Decision Sheet

Watermarking traces a leak; it does not prevent one. It rides inside the picture, so it survives the camera and the re-encode that defeat DRM. Engineering guidance; the standard (ETSI TS 104 002), the MovieLabs ECP, and vendor capabilities change — re-verify live.

1 · PREVENT vs TRACE — THE BOUNDARY

- ☐ **DRM prevents access; the watermark traces the source** after a leak. Run both — never one instead of the other.
- ☐ **The mark rides inside the picture** — it survives screen capture, re-encode, scaling, crop, and HDR→SDR.
- ☐ **It carries a reference number, not a name.** Your back-end maps the ID to a session/subscriber — secure that table.
- ☐ **Watermark ≠ fingerprint**: a fingerprint finds the content in the wild; the watermark blames the session.

2 · THREE INSERTION POINTS

- ☐ **Client-side** — marks on the device. Exposes decrypted video and the secret on an open device. Avoid as primary.
- ☐ **Server-side A/B** — two variants per segment; the network serves a per-session A/B pattern. No device code. ~2× cache.
- ☐ **Edge** — mark per request at the CDN edge. Lowest delivery penalty; needs a watermark-aware edge. Good for live.
- ☐ **Rule of thumb** — the further down the chain you embed, the lower the cost, but the more capable the network must be.

3 · WHEN CONTENT OWNERS REQUIRE IT

- ☐ **Studios (MovieLabs ECP v1.4)** — forensic watermarking for 4K/UHD, HDR, and early-window titles.
- ☐ **Live sport** — to find and cut a pirate re-stream within minutes, while the match still matters.
- ☐ **Standard** — server-side A/B is ETSI TS 104 002 (from DASH-IF); works for both HLS and DASH.
- ☐ **Variants stay encrypted** (Common Encryption) — A/B does not break the secure data path.

4 · READINESS CHECKLIST

- ☐ **Mark only what the contract requires** — doubling variants on unprotected content wastes egress.
- ☐ **Budget delivery, not storage** — A/B doubles cache footprint and lowers CDN hit ratio on your best titles.
- ☐ **Wire the detection loop** — monitoring → extract → session/subscriber → account action + takedown.
- ☐ **Test extraction** against real abuse (screen capture, re-encode, crop); ask vendors how they handle collusion.

THE ONE RULE — WATERMARKING TRACES, IT DOES NOT PREVENT

A forensic watermark does not reduce the number of leaks; it changes a leak from anonymous to attributable. Deploy it alongside encryption and DRM, never instead. Server-side A/B gives every viewer a unique A/B segment pattern from just two variants (ETSI TS 104 002) and keeps the secret out of the open device. Price it as a delivery cost: both variants traverse the CDN, so the cache footprint of marked content doubles and the hit ratio falls — the bill is egress, not disk. For live sport the whole monitor-extract-cut loop races a roughly fifteen-minute window. Robustness, invisibility, and payload trade off, and collusion is a real attack — confirm current standards and vendor capabilities live; they change.