Multi-DRM Integration Reference Pack

The protected-video architecture on one page: one protection boundary and five layers. Encrypt once with cbcs, keep every key inside the boundary, and gate every license. Engineering guidance; specs and vendor capabilities change (ISO/IEC 23001-7, W3C EME, DASH-IF CPIX, PlayReady 4.8 / 2026) — re-verify live.

1 · THE PROTECTION BOUNDARY

- ☐ **Inside** — content keys, key service (KMS), license server, and the entitlement gate. The secrets.
- ☐ **Outside** — encrypted segments on the CDN, the manifest, the player UI. Designed to travel in the open.
- ☐ **The only reach outside your walls** is the device's decryption module (CDM); keys arrive there wrapped.
- ☐ **DRM protects the bytes, not the screen** — a camera pointed at a display is past the boundary.

2 · ENCRYPT ONCE + KEY HANDOFF

- ☐ **Encrypt once with cbcs CENC** (ISO/IEC 23001-7), packaged as CMAF — one encode serves every device.
- ☐ **cenc (AES-CTR) breaks FairPlay**; cbcs plays on all three systems. Decide cbcs on day one or re-encode later.
- ☐ **Keys move via DASH-IF CPIX** (often AWS SPEKE) from the key service to the packager — signed, not by hand.
- ☐ **The key never touches** the player code, the manifest, or the network in the clear.

3 · LICENSE + CLIENT LAYER

- ☐ **One multi-DRM license server** issues Widevine, PlayReady, and FairPlay licenses from the same encode.
- ☐ **License proxy + entitlement gate** check rights, window, region, and concurrency BEFORE a key is issued.
- ☐ **Browser playback uses W3C EME + MSE**; the CDM decrypts out of reach of your code.
- ☐ **Security level controls resolution** — L1 / SL3000 / FairPlay + HDCP 2.2+ for 4K; software DRM is capped to SD.

4 · INTEGRATION READINESS CHECKLIST

- ☐ **cbcs / CMAF chosen** and FairPlay verified on a real Apple device, not just Android/Windows.
- ☐ **CPIX / SPEKE handoff wired**; KMS access locked down; no content key in any client log or manifest.
- ☐ **Proxy + entitlement own the boundary** — every license request passes the rights check first.
- ☐ **Security-level → resolution policy enforced**, with HDCP 2.2+ required for premium tiers.
- ☐ **Watermarking + anti-piracy loop** in place for premium/live; revocation plan ready (PlayReady 4.8, 2026).

THE ONE RULE — ENCRYPT ONCE, KEEP KEYS INSIDE THE BOUNDARY, GATE EVERY LICENSE

A content-protection architecture is one protection boundary plus five layers. The boundary separates the secrets — content keys, the key service, the license server, and the entitlement gate — from the encrypted segments that travel in the open; the only place it reaches outside your walls is the device's decryption module, where keys arrive wrapped. Layer 1 encrypts the catalog once with the cbcs scheme of Common Encryption (ISO/IEC 23001-7) packaged as CMAF, because cenc breaks FairPlay and the fix is a full re-encode. Layer 2 keeps keys in a key service and hands them to the packager through DASH-IF CPIX (often AWS SPEKE), never to the player. Layer 3 issues Widevine, PlayReady, and FairPlay licenses from one encode through a proxy and an entitlement gate that check rights before any key is released. Layer 4 plays through W3C EME, where the device's module decrypts at a security level that sets the resolution — hardware level plus HDCP 2.2+ for 4K. Layer 5 adds forensic watermarking and an anti-piracy operations loop, because protection is a loop, not a wall: it raises the pirate's cost and defends the high-value window, but it does not eliminate piracy.