Common Encryption (CENC) Quick Reference — cenc vs cbcs

Pick your encryption scheme before you lock a packaging config or sign a DRM contract. One encrypted copy can serve all three DRM systems — if you choose the right scheme. Engineering guidance; confirm vendor and device support live, it changes.

1 · THE TWO SCHEMES THAT SHIP

- ☐ **cenc** = AES counter mode (CTR), full subsample. Read by Widevine + PlayReady — NOT FairPlay.
- ☐ **cbcs** = AES chaining mode (CBC), 1:9 video pattern. Read by ALL three: Widevine, PlayReady, FairPlay.
- ☐ **cbc1 / cens / sve1** exist in ISO/IEC 23001-7 but are rare or new — ignore them for planning.
- ☐ **Not interchangeable:** a device reads only the scheme its DRM supports. Wrong scheme = black screen.

2 · THE RULE — cbcs EVERYWHERE

- ☐ **Standardize on cbcs in CMAF** — one encrypted master serves Widevine, PlayReady, and FairPlay.
- ☐ **cenc-only packaging shows a BLACK SCREEN on every Apple device** — FairPlay cannot read cenc.
- ☐ **Add a cenc copy ONLY** for a specific old-device tail that predates cbcs — deliberate, not default.
- ☐ **Test on real hardware** from all three ecosystems before launch — not just Chrome.

3 · THE FOUR SIGNALING BOXES

- ☐ **schm** — declares the scheme (cenc or cbcs). The player reads this first.
- ☐ **tenc** — default encryption params + default_KID (the 128-bit NAME of the key, not the key).
- ☐ **senc** — per-sample initialization vectors (IVs) and subsample ranges.
- ☐ **pssh** — one per DRM system (Widevine / PlayReady / FairPlay); each device reads its own.

4 · PACKAGING DECISION

- ☐ **Default — encrypt once:** cbcs + CMAF → all three DRMs. Scheme chosen: _____
- ☐ **Legacy tail only:** add a second cenc copy, using a DIFFERENT content key.
- ☐ **Never mix** cenc and cbcs inside one set of switchable renditions.

WHY FAIRPLAY DECIDES THE DEFAULT

Apple built HLS on SAMPLE-AES, which encrypts samples with AES in cipher-block-chaining (CBC) mode. When pattern encryption entered Common Encryption (ISO/IEC 23001-7) in 2016, Apple's CBC approach mapped onto the cbcs scheme — so every iPhone, iPad, Mac, and Apple TV reads ONLY cbcs and cannot read the counter-mode cenc at all. Modern Widevine and PlayReady read both schemes. That makes cbcs the single scheme all three systems accept, which is why you standardize on it. Bonus: the cbcs 1:9 pattern encrypts only about one block in ten, cutting decrypt work to roughly a tenth — the reason 4K plays smoothly on phones. Confirm current device support; it changes.