Access-Control Readiness Checklist — One-Page Reference

Fora Soft Learn

The paywall is a screen; access control is the system that decides and enforces every play. Pick a paywall shape on purpose, then enforce in four server-side layers. Engineering guidance; vendor limits and case law change in 2026 — confirm live.

1 · PICK THE PAYWALL SHAPE (on purpose)

- ☐ **Hard** — pay to watch anything; max revenue/user, hardest first impression. Premium catalogs.
- ☐ **Metered / soft** — a free quota (e.g. 3/month), then pay; buys habit, reach, and SEO.
- ☐ **Freemium** — a permanent free tier as marketing for a paid one; pairs with a registration wall.
- ☐ **Registration wall** — email/account is the price; collect first-party data (mind the VPPA, col. 4).

2 · ENFORCE IN FOUR SERVER-SIDE LAYERS

- ☐ **Entitlement check** — on every play: may this account watch this title, in this region, now?
- ☐ **Signed token (JWT)** — proves the decision; carries user/asset/region claims + a short expiry.
- ☐ **Signed delivery URL** — CDN serves bytes only to a valid signature; 60-300 s segment lifetime.
- ☐ **DRM license** — encrypts the content; the only layer that protects the decrypted video.

3 · GEO-GATING + CONCURRENCY

- ☐ **Geo-gate** — resolve country by IP; enforce the title's territorial license at the edge.
- ☐ **EU portability** ((EU) 2017/1128) — let a paying subscriber watch home content while temporarily in the EU.
- ☐ **Device ≠ residence** — portability keys off the subscriber's home market, not current location.
- ☐ **Concurrency** — heartbeat every 30-60 s; refuse plays over the plan cap; reclaim crashed slots.

4 · VPPA / CONSENT CHECKLIST (registration walls)

- ☐ **Separate consent** — get explicit, informed consent to SHARE viewing data; a cookie banner is not enough.
- ☐ **No leaky pixels** — keep video-viewing events out of ad pixels (Meta/Google) you do not control.
- ☐ **Auditable record** — store the consent as queryable data; $2,500 minimum statutory damages per violation.
- ☐ **Watch the case law** — Salazar v. Paramount is live at SCOTUS (2026); re-check before launch.

BUILD ORDER — ONLY THE SERVER MAY DECIDE WHAT TO SERVE

Never enforce the gate in the client: an app check is one line edited in the console, and the video files sit on a CDN behind URLs anyone can fetch if they are unsigned. The client may hide the Play button for a better experience, but the entitlement check, the signed playback token (JWT, RFC 7519), the signed delivery URL, and the DRM license must all be enforced server-side and at the edge, where the user cannot reach them. Keep tokens short (60-300 s for segment URLs) so a leaked URL dies before it can be shared. The test: imagine the most hostile user has your raw segment URLs, a patched app, and a VPN — if your revenue still holds, the gate is real. Re-verify per-service concurrency limits and VPPA case law before launch; both move in 2026.