

Как плеер получает ключ для расшифровки — и где обязан остаться каждый секрет. Зашифрованное видео бесполезно без ключа; вся задача — доставить его нужному устройству на одно воспроизведение и больше никуда. Инженерное руководство; поддержку вендоров и устройств сверяйте вживую, она меняется.

1 · ПОТОК ПОЛУЧЕНИЯ ЛИЦЕНЗИИ (ЕМЕ)

- ☐ **encrypted -> generateRequest()** — плеер открывает сессию ключей и просит CDM собрать запрос.
- ☐ **message** — CDM выдаёт подписанный устройством запрос лицензии; приложение (JS) везёт его, не читая.
- ☐ **POST + токен прав** — приложение пересылает запрос на сервер лицензий с коротким токеном.
- ☐ **update()** — сервер возвращает ключ, завёрнутый под устройство; ключ оказывается в CDM. Видео играет.

2 · КАРТА СЕКРЕТОВ — КТО НЕ ВИДИТ КЛЮЧ НИКОГДА

- ☐ **Контент-ключ (СЕК)** открыт ТОЛЬКО в: KMS/HSM, сервере лицензий и CDM/TEE устройства. Больше нигде.
- ☐ **default_KID** — публичное ИМЯ ключа, его можно класть в манифест. Не путайте имя с самим ключом.
- ☐ **Ключ связи** (сервис прав ↔ сервер лицензий) НИКОГДА не уезжает в клиент — утечёт = штампуют токены.
- ☐ **Никогда** не кладите открытый ключ в манифест, на CDN, в JS-плеер или в логи.

ЗАЧЕМ ЛИЦЕНЗИОННЫЙ ПРОКСИ — ПОСЛЕДНЯЯ ДВЕРЬ К КЛЮЧУ

Сервер лицензий умеет выдать ключ; решать, КОМУ его выдавать, — ваш сервис прав, и жить он обязан на сервере. Чистый паттерн — лицензионный прокси: плеер шлёт запрос без секрета; прокси проверяет подписку, регион и лимит одновременных потоков, выпускает свежий одноразовый токен (секунды, не часы) и пересылает запрос настоящему серверу лицензий. Проверку прав в JavaScript-плеере обходит любой, кто откроет инструменты разработчика; ключ связи в клиенте даёт злоумышленнику штамповать валидные токены от вашего имени. Держите права на сервере, токены — короткими и одноразовыми, и плеер видит эндпоинт, который всегда отвечает. Сверяйте актуальную поддержку вендоров; она меняется.

3 · ТРИ ДИАЛЕКТА

- ☐ **Widevine** — CDM шлёт подписанный **запрос лицензии**; сервер возвращает лицензию. Android, Chrome, TB.
- ☐ **PlayReady** — клиент шлёт **license challenge** (XML) + KID; сервер возвращает лицензию. Windows, Xbox, TB.
- ☐ **FairPlay** — устройство шлёт **SPC**; KSM сверяет сертификат и возвращает **СКС** с ключом. Только Apple.
- ☐ **Multi-DRM** говорит на всех трёх из одной упаковки cbcs — один воркфлоу, любое устройство.

4 · ТИПЫ СЕССИЙ И РОТАЦИЯ В ЭФИРЕ

- ☐ **temporary** — лицензия умирает с вкладкой; умолчание для онлайн. Секрета на диске нет.
- ☐ **persistent-license** — пишется на диск для ОФЛАЙН-просмотра; осознанный секрет на диске, правила строже.
- ☐ **Ротация ключей (эфир)** — меняйте контент-ключ по интервалу; доставляйте ключи пачками (иерархически), иначе пик устроит DDoS вашему серверу лицензий.