Чек-лист hardening подписанных URL

12 пунктов для проверки до запуска платного стриминга.

Используйте этот чек-лист при проектировании нового signed-URL решения, аудите существующего или миграции между CDN. Каждый пункт связан с конкретным артефактом: поле конфига, политика cache key, панель дашборда, правило firewall на origin. Если артефакт не показывается — пункт не сделан.

- ☐ **1. Выбран алгоритм подписи и описана ротация ключей**
  HMAC-SHA256 для Akamai / Google / Fastly / NGINX; RSA-SHA256 (RS256 JWT) для CloudFront / Mux / Cloudflare Stream.
  RSA позволяет менять проверяющий ключ отдельно; HMAC дешевле, но смена общего секрета требует одновременного обновления всех подписывающих.

- ☐ **2. Решено: signed URL или signed cookie — на каждой поверхности**
  Master playlist: signed URL для bootstrap. Variants, сегменты, ключи: signed cookie на защищённый путь.
  Гибрид — стандарт продакшена. Подписывать каждый запрос — убийца экономики кэша.

- ☐ **3. Параметры подписи убраны из cache key**
  Проверьте, что Policy, Signature, Key-Pair-Id (CloudFront) и hdnts (Akamai) исключены из cache key.
  Если подпись попала в cache key, hit ratio падает почти до нуля, а egress на origin резко растёт.

- ☐ **4. Подписывается префикс пути, а не каждый URL**
  Используйте ACL или wildcard (например /customer42/title-9000/*). Одна подпись — все сегменты, стабильный cache key.
  Это же лечит провал переключения битрейта в hls.js (issue #1450).

- ☐ **5. Expiry токена покрывает самую длинную сессию**
  VOD ≤ длительность + 30 мин. Live ≥ длительность события + 30 мин. Долгие сессии должны обновлять токен на лету.
  Через бэкенд + xhrSetup в hls.js или endpoint Set-Cookie для refresh.

- ☐ **6. Токен привязан не только к expiry**
  Подпишите policy с IP CIDR, user ID, отпечатком устройства или session ID — хотя бы что-то помимо метки времени.
  Только timestamp оставляет окно для replay-атак.

- ☐ **7. Учтена ловушка IPv6 (CloudFront)**
  Custom-policy IP в CloudFront — только v4. Отключите IPv6 на distribution или уберите IP-claim из policy.
  При выкатке на iOS-операторах с IPv6-only это всплывает в проде тихо.

- ☐ **8. Origin принимает только трафик CDN**
  Origin Access Control (AWS S3), Authenticated Origin Pulls (Cloudflare), Site Shield (Akamai) или custom shared-secret header.
  Без lockdown URL origin находится одним whois-запросом и скрейпится.

- ☐ **9. Mutual TLS между CDN и origin на платном тарифе**
  CDN предъявляет клиентский сертификат, origin валидирует. Все легальные запросы проходят через CDN-пайплайн.
  Поддерживается enterprise-тарифами всех крупных CDN; стандарт для платных OTT-стэков.

- ☐ **10. max-age кэша ≤ срока подписи для платного контента**
  Если max-age больше expiry, CDN отдаёт закэшированный 200 после того, как токен в исходной URL истёк.
  Либо короткий max-age, либо cookie-сессии, где временной лимит несёт сама cookie.

- ☐ **11. Ключ подписи никогда не покидает сервер**
  Подпись делается на бэкенде, в edge-функции или в KMS. Никогда не во фронтенд-JavaScript или мобильном бандле.
  Фронтенд-секреты появляются в view-source, при декомпиляции приложения или в трейсах прокси за часы после релиза.

- ☐ **12. Observability покрывает режимы отказа**
  Дашборды: 403 rate по шаблону URL, события rebuffer из-за expiry, hit ratio для signed-путей, egress origin по referrer.
  Если плеер видит больше 0,5% 403 на сегментах — у вас баг в токене или cache key.