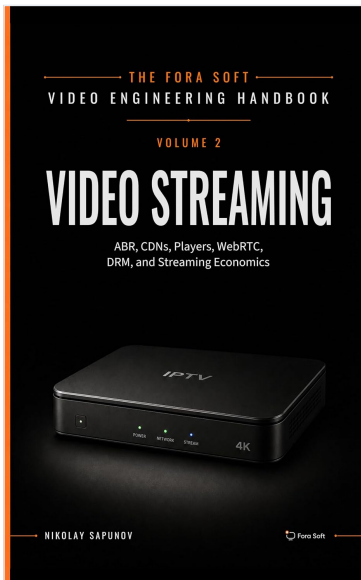


Signed URL Hardening Checklist

12 items to verify before a paid-streaming launch goes live.

Use this checklist when scoping a new signed-URL deployment, auditing an existing one, or migrating between CDNs. Every item maps to a concrete artefact: a config field, a cache-key policy, a dashboard panel, an origin firewall rule. If you cannot point at the artefact, the item is not done.

- ☐ **1. Choose a signing algorithm and document key rotation**
HMAC-SHA256 for Akamai/Google/Fastly/NGINX; RSA-SHA256 (RS256 JWT) for CloudFront/Mux/Cloudflare Stream.
RSA lets you rotate the verifier independently; HMAC is cheaper but rotating the shared secret needs every signer updated at once.
- ☐ **2. Decide signed URL vs signed cookie per surface**
Master playlist: signed URL bootstrap. Variants + segments + keys: signed cookie covering the protected path.
Hybrid is the production default. Pure URL signing on every fetch is the cache-economy killer.
- ☐ **3. Strip signature parameters from the cache key**
Verify Policy, Signature, Key-Pair-Id (CloudFront) and hdnts (Akamai) are excluded from the cache key.
If a signature ends up in the cache key, hit ratio collapses to near zero and origin egress spikes.
- ☐ **4. Sign a path prefix, not every URL**
Use an ACL or wildcard (e.g. /customer42/title-9000/*). One signature, all segments, stable cache key.
This is also what fixes the hls.js bitrate-switch token-expiry failure mode (issue #1450).
- ☐ **5. Token expiry matches the longest plausible session**
VOD $\leq$ runtime + 30 min. Live $\geq$ event duration + 30 min. Sessions long enough to break should refresh mid-stream.
Plan token-renewal via app server + xhrSetup in hls.js, or a Set-Cookie refresh endpoint.
- ☐ **6. Pin the token to user identity, not just expiry**
Bind the policy to IP CIDR, user ID, device fingerprint, or session ID — at least one beyond the timestamp.
Pure timestamp-only tokens enable replay attacks within the validity window.
- ☐ **7. Watch the IPv6 trap (CloudFront)**
CloudFront custom-policy IP restriction is IPv4-only. Disable IPv6 on the distribution, or omit the IP claim.
iOS rollouts on IPv6-only carriers expose this silently in production.
- ☐ **8. Origin allows only CDN traffic**
Origin Access Control (AWS S3), Authenticated Origin Pulls (Cloudflare), Site Shield (Akamai), or a custom shared-secret header.
Without origin lockdown, the origin URL is one whois lookup away from being scraped.
- ☐ **9. Mutual TLS between CDN and origin for paid tier**
CDN presents a client certificate; origin validates it. Forces every legitimate request through the CDN pipeline.
Enterprise tier on every major CDN supports this; it is the default for OTT paid stacks.
- ☐ **10. Cache max-age $\leq$ signature validity for paid content**
If max-age > expiry, the CDN serves a cached 200 after the original token has expired.
Either keep max-age short or rely on cookie-bound sessions where the cookie carries the time bound.
- ☐ **11. Signing secret never leaves the server**
Generate signatures in a backend service, edge function, or KMS. Never in front-end JavaScript or mobile bundle.
Front-end secrets show up in view-source, app decompilation, or proxy traces within hours of launch.
- ☐ **12. Observability covers the failure modes**
Dashboards: 403 rate by URL pattern, token-expiry rebuffer events, cache hit ratio for signed paths, origin egress by referrer.
If a player sees more than 0.5% 403s on segments, a token or cache-key bug is in flight.



GO DEEPER · VOLUME 3 OF 7

Video Streaming: A Complete Guide to Video Delivery

From ABR and CDNs to Players, WebRTC, DRM, and the Economics of Streaming

By Nikolay Sapunov, CEO at Fora Soft · 1,182 pages · Kindle & paperback on Amazon

[Read it on Amazon →](#)
amazon.com/dp/B0HH76ZYWC

This checklist covers signing algorithms, cache keys, token expiry, origin lockdown and the observability you need before a paid launch. Volume 3 covers CDN delivery and caching in depth, along with DRM, players and the economics of streaming traffic.

WHAT YOU WILL FIND INSIDE

- CDN caching and cache-key design
- DRM and content protection
- Players and token renewal
- Delivery economics and egress cost

THE FULL HANDBOOK · 7 VOLUMES · 9,000+ PAGES · ALL ON AMAZON

Vol. 1 · Video Encoding — pixels and color to H.264, HEVC, AV1, quality metrics and AI

Vol. 2 · Video Streaming I — network transport, contribution and ingest, HLS, MPEG-DASH, CMAF

Vol. 3 · Video Streaming II — ABR, CDNs, players, WebRTC, DRM and the economics of delivery

Vol. 4 · Audio for Video I — PCM, codecs, loudness, accessibility, real-time voice processing

Vol. 5 · Audio for Video II — jitter buffers, lip sync, Atmos, quality metrics, neural codecs

Vol. 6 · AI for Video I — models and inference, computer vision, speech, search, generative video

Vol. 7 · AI for Video II — real-time pipelines, agents, serving, cost, compliance, verticals

Launching paid streaming and worried about stream theft?

We will design token and cache-key policies per CDN, lock the origin, and set up dashboards that catch 403 spikes before viewers do. 250+ video products shipped since 2005.

[Book a 30-min call →](#)
[WhatsApp →](#)
[Email us →](#)