

Streaming Encryption Configuration Checklist

Companion to: DTLS, SRTP, TLS, mTLS — The Encryption Layer for Media

1 · TLS 1.3 for HTTPS surfaces

Every HLS, DASH, dashboard, and signalling endpoint.

- ☐ Prefer TLS 1.3 (RFC 8446); allow TLS 1.2 only for long-tail clients.
- ☐ Disable TLS 1.0 / 1.1 entirely — formally deprecated by RFC 8996.
- ☐ Enable HSTS with max-age=31536000 and includeSubDomains.
- ☐ Use 0-RTT only on idempotent segment GETs, never on POSTs.
- ☐ Roll out Encrypted Client Hello (RFC 9849) where the CDN supports it.

2 · DTLS 1.3 for WebRTC

Handshake before any SRTP packet flows.

- ☐ Negotiate DTLS 1.3 (RFC 9147) preferred, DTLS 1.2 minimum.
- ☐ Reject DTLS 1.0 / 1.1 outright in your media-server config.
- ☐ Use ECDSA P-256 or Ed25519 for the self-signed cert.
- ☐ Bind the cert to SDP via a=fingerprint: per RFC 8842.
- ☐ Generate a fresh handshake per session; never reuse SRTP keys.

3 · SRTP cipher and integrity

Per-packet encryption of every RTP frame.

- ☐ Default to AES-128-GCM per RFC 7714; avoid AES-CM with HMAC-SHA1.
- ☐ SRTCP integrity is mandatory (RFC 3711 §3.4) — never disable.
- ☐ Confirm AES-NI is available on every media server CPU.
- ☐ Account for ~16 kbps auth overhead on a 2 Mbps stream.
- ☐ Verify keys derive from the RFC 5705 exporter, not a manual KDF.

4 · mTLS where identity matters

Both sides present a certificate.

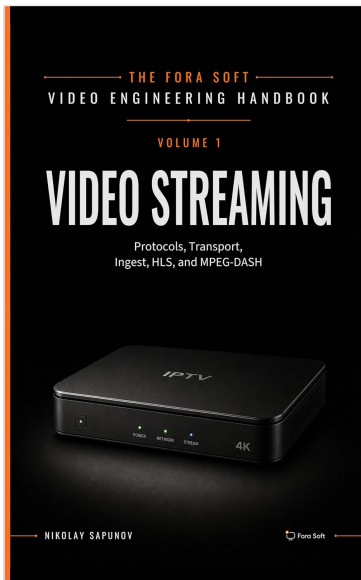
- ☐ Ingest encoders: SRT-over-TLS or RTMPS with client cert.
- ☐ CDN to origin: turn on origin mTLS (e.g. CloudFront, Feb 2026).
- ☐ Service mesh: Istio / Linkerd / SPIRE with 24-hour certs.
- ☐ Trust only a private CA scoped to the streaming product.
- ☐ Automate cert rotation; alert when any cert is <14 days from expiry.

Audit questions you will be asked in every enterprise security review

1 · Which TLS versions does your service accept, and how are TLS 1.0/1.1 actively rejected? 2 · Are HLS / DASH segments served exclusively over HTTPS, with HSTS, and is mixed content blocked at the player? 3 · Which DTLS versions and cipher suites does your media server negotiate, and what is the cutover plan to DTLS 1.3?

4 · Is SRTP using AES-GCM, and is SRTCP integrity enabled on every session? 5 · How are DTLS-SRTP keys derived per session, and are session certs rotated? 6 · Where in the pipeline is mTLS enforced — ingest, CDN-origin, service-to-service?

Controlling specs: RFC 8446 (TLS 1.3) · RFC 9147 (DTLS 1.3) · RFC 5764 (DTLS-SRTP) · RFC 3711 + RFC 7714 (SRTP, AES-GCM) · RFC 8827 (WebRTC Security Architecture) · RFC 8842 (SDP-DTLS fingerprint) · RFC 9849 (Encrypted Client Hello, March 2026).



GO DEEPER · VOLUME 2 OF 7

Video Streaming: A Complete Guide to Video Delivery

From Network Protocols and Transport to Ingest, HLS, and MPEG-DASH

By Nikolay Sapunov, CEO at Fora Soft · 1,124 pages · Kindle & paperback on Amazon

Read it on Amazon →

amazon.com/dp/B0HH8F4R82

This checklist sets TLS 1.3, DTLS, SRTP and mTLS correctly across ingest, delivery and WebRTC. Volume 2 covers the transport layer these settings live on: TCP and UDP behaviour, QUIC and HTTP/3, NAT traversal and secure contribution with RTMPS, SRT and RIST.

WHAT YOU WILL FIND INSIDE

- QUIC and HTTP/3 and how they carry TLS 1.3
- UDP transport, NAT traversal and what DTLS runs over
- Secure contribution: RTMPS, SRT encryption and RIST
- Ingest paths from encoder to origin

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

Preparing your streaming platform for an enterprise security review?

We will audit your TLS, DTLS-SRTP and mTLS setup end to end and hand you the answers security reviewers ask for, with fixes applied. 250+ video products shipped since 2005.

Book a 30-min call →

WhatsApp →

Email us →