

WebRTC Security Pre-Flight Checklist

28 items to verify before shipping a WebRTC product — DTLS, SRTP, fingerprints, signalling, SFrame

1. Signalling channel

- ☐ Signalling endpoint is **wss://** (or HTTPS), never plain ws:// or http://.
- ☐ TLS certificate on the signalling server passes a public-CA chain — not self-signed in production.
- ☐ WebSocket origin is restricted server-side to the app's domain — block cross-origin signalling clients.
- ☐ Per-connection authentication: short-lived bearer token (JWT or equivalent) verified server-side before any SDP is relayed.

2. DTLS handshake

- ☐ Browser supports **DTLS 1.3** (RFC 9147) — verify in chrome://webrtc-internals or about:webrtc.
- ☐ DTLS 1.0 / 1.1 disabled on the SFU side; only 1.2 and 1.3 accepted.
- ☐ Cipher suite list excludes weak/deprecated AES-CBC modes; AEAD-only enforced.
- ☐ Self-signed cert lifetime matches the PeerConnection lifetime — verify cert is regenerated per connection.

3. SRTP profile

- ☐ **AEAD-AES-128-GCM** negotiated as the preferred SRTP profile (RFC 7714).
- ☐ Legacy AES-CM-HMAC-SHA1-80 accepted only as a fallback; logs flagged when used.
- ☐ Replay window is at default (64 packets) or larger; not disabled.
- ☐ Authentication tags present on every media packet — verify a sample with Wireshark.

4. SDP fingerprint

- ☐ **a=fingerprint:sha-256** present in every offer and every answer.
- ☐ SHA-1 fingerprints rejected by the application — log and fail the negotiation.
- ☐ Fingerprint mismatch handling: connection torn down, error surfaced to user.

5. ICE & privacy

- ☐ **mDNS host candidates** used by the client (default in modern Chromium / Edge / Opera).
- ☐ TURN server requires short-lived ephemeral credentials (REST-over-HTTPS, expiring < 1 hour).
- ☐ TURN-relay rate measured in production telemetry — typical 10–15%; spikes flagged.
- ☐ Public IP exposure documented and disclosed in privacy policy.

6. Identity & authorization

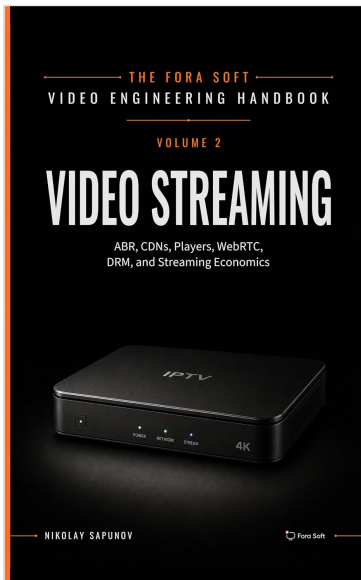
- ☐ SFU enforces token-bound room access — publisher and subscriber tokens verified before media flow.
- ☐ Per-track permissions (publish vs subscribe) decided server-side, not by the client.
- ☐ Token expiration short enough to limit replay (15–60 minutes typical).
- ☐ Rotation policy documented for SFU API keys and JWT signing keys.

7. E2EE (if claimed)

- ☐ SFrame (RFC 9605) implemented on top of Insertable Streams if the product claims E2EE through an SFU.
- ☐ Group-key management documented — MLS, bespoke, or vendor-provided.
- ☐ Key rotation on join/leave is tested with at least one chaos-test scenario.
- ☐ Browser support boundaries documented (Safari/Firefox Insertable Streams gaps in 2026).

8. Observability

- ☐ DTLS handshake failures alerted on with reason code (cert mismatch, version, cipher suite).
- ☐ SDP-fingerprint-mismatch events emitted to security log and dashboarded.
- ☐ RTT and TURN-relay rate per session retained for at least 30 days for forensics.



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 signalling, DTLS, SRTP, fingerprints, identity and E2EE before a WebRTC launch. Volume 3 covers the delivery side of that security in depth: WebRTC and real-time delivery, DRM and content protection, QoE monitoring and the cost of every protection layer.

WHAT YOU WILL FIND INSIDE

- WebRTC and real-time delivery
- QoE monitoring
- DRM and content protection
- Economics of delivery

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 a WebRTC product for a security review?

We will audit signalling, DTLS and SRTP settings, token flows and E2EE claims, and hand you a list of fixes ranked by risk. 250+ video products shipped since 2005.

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