Чек-лист конфигурации шифрования стриминга

К статье «DTLS, SRTP, TLS, mTLS: слой шифрования для медиа»

1 · TLS 1.3 для HTTPS-поверхностей

Каждый эндпоинт HLS, DASH, дашборда и сигналинга.

- ☐ Предпочитайте TLS 1.3 (RFC 8446); TLS 1.2 — только как фолбэк.
- ☐ Полностью отключите TLS 1.0 / 1.1 — формально устарели по RFC 8996.
- ☐ Включите HSTS с max-age=31536000 и includeSubDomains.
- ☐ 0-RTT только на идемпотентных GET-запросах за сегментами.
- ☐ Раскатывайте Encrypted Client Hello (RFC 9849), где CDN поддерживает.

2 · DTLS 1.3 для WebRTC

Handshake до любого SRTP-пакета.

- ☐ Согласуйте DTLS 1.3 (RFC 9147) предпочтительно, DTLS 1.2 — минимум.
- ☐ Отклоняйте DTLS 1.0 / 1.1 прямо в конфиге media-сервера.
- ☐ Используйте ECDSA P-256 или Ed25519 для самоподписанного cert.
- ☐ Привяжите cert к SDP через a=fingerprint: по RFC 8842.
- ☐ Генерируйте свежий handshake на каждую сессию; никогда не переисп. ключи SRTP.

3 · Шифр SRTP и целостность

Шифрование каждого RTP-пакета.

- ☐ Дефолт AES-128-GCM по RFC 7714; избегайте AES-CM с HMAC-SHA1.
- ☐ Целостность SRTCP обязательна (RFC 3711 §3.4) — не отключать.
- ☐ Подтвердите наличие AES-NI на каждом media-сервере.
- ☐ Учтите ~16 kbps накладных расходов на 2 Mbps-потоке.
- ☐ Ключи выводите через exporter RFC 5705, не вручную.

4 · mTLS там, где важна идентичность

Сертификат предъявляют обе стороны.

- ☐ Ingest-энкодеры: SRT-over-TLS или RTMPS с клиентским cert.
- ☐ CDN — origin: включите origin mTLS (CloudFront — фев. 2026).
- ☐ Service mesh: Istio / Linkerd / SPIRE с 24-часовыми cert.
- ☐ Доверяйте только приватному CA, ограниченному стриминг-продуктом.
- ☐ Автоматизируйте ротацию; алерт за <14 дней до истечения cert.

Аудит-вопросы, которые задают в каждом энтерпрайзном security review

1 · Какие версии TLS принимает сервис, как активно отклоняются TLS 1.0 / 1.1? 2 · Все ли HLS / DASH-сегменты отдаются исключительно по HTTPS с HSTS, блокируется ли mixed content на плеере? 3 · Какие версии DTLS и шифронаборы согласует media-сервер, каков план перехода на DTLS 1.3?

4 · Использует ли SRTP шифр AES-GCM, включена ли целостность SRTCP в каждой сессии? 5 · Как выводятся ключи DTLS-SRTP на сессию, ротируются ли сессионные cert? 6 · Где в pipeline'е принудительно включён mTLS — ingest, CDN-origin, service-to-service?

Управляющие спецификации: 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, март 2026).