

Common Encryption (CENC): краткий справочник — cenc vs cbcs

Fora Soft Learn

Выберите схему шифрования до фиксации конфигурации упаковки и до подписания контракта на DRM. Одна зашифрованная копия может обслужить все три системы DRM — если выбрать верную схему. Инженерное руководство; поддержку вендоров и устройств сверяйте вживую, она меняется.

1 · ДВЕ СХЕМЫ, КОТОРЫЕ РЕАЛЬНО ПРИМЕНЯЮТСЯ

- ☐ **cenc** = AES counter mode (CTR), полное subsample-шифрование. Читают Widevine + PlayReady — HE FairPlay.
- ☐ **cbcs** = AES chaining mode (CBC), паттерн 1:9 для видео. Читают BCE три: Widevine, PlayReady, FairPlay.
- ☐ **cbcs1 / cenc / sve1** есть в ISO/IEC 23001-7, но редки или новы — при планировании игнорируйте.
- ☐ **Несовместимы:** устройство читает только схему своего DRM. Неверная схема = чёрный экран.

2 · ПРАВИЛО — cbcs ВЕЗДЕ

- ☐ **Стандартизируйтесь на cbcs в CMAF** — один зашифрованный мастер для Widevine, PlayReady и FairPlay.
- ☐ **Упаковка только в cenc даёт ЧЁРНЫЙ ЭКРАН на всех устройствах Apple** — FairPlay не читает cenc.
- ☐ **Добавляйте копию cenc ТОЛЬКО** для старых устройств без cbcs — осознанно, а не по умолчанию.
- ☐ **Тестируйте на реальном железе** всех трёх экосистем до запуска — не только в Chrome.

ПОЧЕМУ FAIRPLAY ЗАДАЁТ СХЕМУ ПО УМОЛЧАНИЮ

Apple построила HLS на SAMPLE-AES, где сэмплы шифруются AES в режиме сцепления блоков (CBC). Когда в 2016 году в Common Encryption (ISO/IEC 23001-7) добавили pattern-шифрование, подход Apple на CBC лёг на схему cbcs — поэтому каждый iPhone, iPad, Mac и Apple TV читает ТОЛЬКО cbcs и совсем не понимает counter-mode cenc. Современные Widevine и PlayReady читают обе схемы. Значит, cbcs — единственная схема, понятная всем трём системам, поэтому на ней и стандартизируются. Бонус: паттерн 1:9 в cbcs шифрует лишь примерно один блок из десяти, снижая работу при расшифровке почти в 10 раз — поэтому 4K плавно играет на телефонах. Сверяйте актуальную поддержку устройств; она меняется.

3 · ЧЕТЫРЕ БОКСА СИГНАЛИЗАЦИИ

- ☐ **schm** — объявляет схему (cenc или cbcs). Плеер читает его первым.
- ☐ **tenc** — параметры шифрования по умолчанию + default_KID (128-битное ИМЯ ключа, не сам ключ).
- ☐ **senc** — векторы инициализации (IV) и диапазоны subsample для каждого сэмпла.
- ☐ **pssh** — по одному на систему DRM (Widevine / PlayReady / FairPlay); каждое устройство читает свой.

4 · РЕШЕНИЕ ПО УПАКОВКЕ

- ☐ **По умолчанию — шифруем один раз:** cbcs + CMAF → все три DRM. Выбранная схема: _____
- ☐ **Только для старых устройств:** добавьте вторую копию cenc с ДРУГИМ контент-ключом.
- ☐ **Никогда не смешивайте** cenc и cbcs внутри одного набора переключаемых рендиций.