

CENC — справочник

ISO/IEC 23001-7 на одной странице — схемы защиты, метаданные-боксы, System ID и четыре ловушки.

Схемы защиты (ISO/IEC 23001-7:2023)

Схема	Режим шифра	Паттерн	Где используется	Статус в 2026
cenc	AES-128 CTR	Полное покрытие подсэмпла	Легаси DASH-only	Дефолт до 2018 — уходит
cbcs	AES-128 CBC	1 из 10 (crypt=1, skip=9)	FairPlay требует; принимают Widevine и PlayReady	Продакшен-дефолт для новых пайплайнов
cbc1	AES-128 CBC	Полное покрытие подсэмпла	Определена; не используется	Практически не встречается
cens	AES-128 CTR	1 из 10	Определена; не используется	Практически не встречается

Четыре CENC-бокса метаданных, которые нужно знать

Бокс	Расположение	Что несёт
schm	moov/.../sinf/schm	Четырёхбуквенный тег схемы: cenc, cbcs, cens, cbc1
tenc	moov/.../sinf/schi/tenc	default_KID, размер IV по умолчанию, параметры паттерна
pssh	moov/pssh или <cenc:pssh> в MPD	По одному на DRM — SystemID + DRM-специфичный payload
senc	moof/traf/senc (на фрагмент)	Per-sample IV и счётчики байтов подсэмплов

System ID DRM (реестр DASH-IF)

Widevine · edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
PlayReady · 9a04f079-9840-4286-ab92-e65be0885f95
FairPlay · 94ce86fb-07ff-4f43-adb8-93d2fa968ca2
W3C Common · 1077efec-c0b2-4d02-ace3-3c1e52e2fb4b

Каждый pssh-бокс называет ровно один System ID.

Сигнализация в манифесте

HLS EXT-X-KEY METHOD=SAMPLE-AES + KEYFORMAT.
com.apple.streamingkeydelivery → FairPlay.

DASH <ContentProtection> на AdaptationSet:
schemeIdUri=urn:mpeg:dash:mp4protection:2011
value="cbcs" · cenc:default_KID="..."
Плюс по одному на DRM, с дочерним <cenc:pssh>.

Четыре ловушки

- 1. Шифрование только cenc → нет FairPlay.
- 2. Порядок байт default_KID не совпадает (MS GUID).
- 3. pssh только в moov, а не в MPD — тяжёлый CDN-сброс.
- 4. Один контентный ключ на весь каталог.

Решение в одну строку

Шифруйте один раз по cbcs. Подписывайте под HLS и DASH с одного набора CMAF-сегментов. pssh-данные кладите в манифест, а не в init-сегмент.