CENC Quick Reference

ISO/IEC 23001-7 in one page — protection schemes, metadata boxes, DRM System IDs, and the four pitfalls.

Protection schemes (ISO/IEC 23001-7:2023)

Scheme	Cipher mode	Pattern	Where it ships	Status in 2026
cenc	AES-128 CTR	Full subsample	Legacy DASH-only	Pre-2018 default — fading
cbcs	AES-128 CBC	1 of 10 (crypt=1, skip=9)	FairPlay-required, accepted by Widevine + PlayReady	Production default for new pipelines
cbc1	AES-128 CBC	Full subsample	Defined; not deployed	Effectively unused
cens	AES-128 CTR	1 of 10	Defined; not deployed	Effectively unused

Four CENC metadata boxes you must know

Box	Location	What it carries
schm	moov/.../sinf/schm	Four-letter scheme tag: cenc, cbcs, cens, cbc1
tenc	moov/.../sinf/schi/tenc	default_KID, default IV size, pattern parameters
pssh	moov/pssh or MPD <cenc:pssh>	One per DRM — SystemID + DRM-specific payload
senc	moof/traf/senc (per fragment)	Per-sample IVs and subsample byte counts

DRM System IDs (DASH-IF registry)

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

Each pssh box names exactly one System ID.

Manifest signalling

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

DASH <ContentProtection> on the AdaptationSet:
schemeIdUri=urn:mpeg:dash:mp4protection:2011
value="cbcs" · cenc:default_KID="..."
Plus one per DRM, with <cenc:pssh> child.

Four pitfalls

1. cenc-only encryption → locked out of FairPlay.
2. default_KID byte-order mismatch (MS GUID vs ISO).
3. pssh only in moov, not in MPD — hard CDN invalidation.
4. Same content key for the whole catalogue.

Decision in one line

Encrypt once with cbcs. Sign for HLS and DASH off one set of CMAF segments. Place pssh data in the manifest, not the init segment.