noisypeak

THE APEX OF VIDEO OVER IP SOLUTIONS

CONTENT PROTECTION · PRODUCT BROCHURE

Noisypeak DRM

Multi-DRM packaging, tokenised delivery and forensic watermarking on one encoding and origin pipeline.



Noisypeak DRM encrypts one HLS/DASH packaging for FairPlay, Widevine, PlayReady, Verimatrix and Nagra inside the UEN2 encoder, gates delivery with JWT tokens and access lists at the origin, and adds forensic watermarking that survives camripping — so a leak can be traced to its source.

5
DRM SYSTEMS · FAIRPLAY, WIDEVINE, PLAYREADY, VERIMATRIX, NAGRA

RFC 7519
JWT LINK TOKENIZATION AT THE ORIGIN

2,500
PARALLEL STREAMS PER ORIGIN NODE

20 Gb/s
SUSTAINED DELIVERY PER NODE

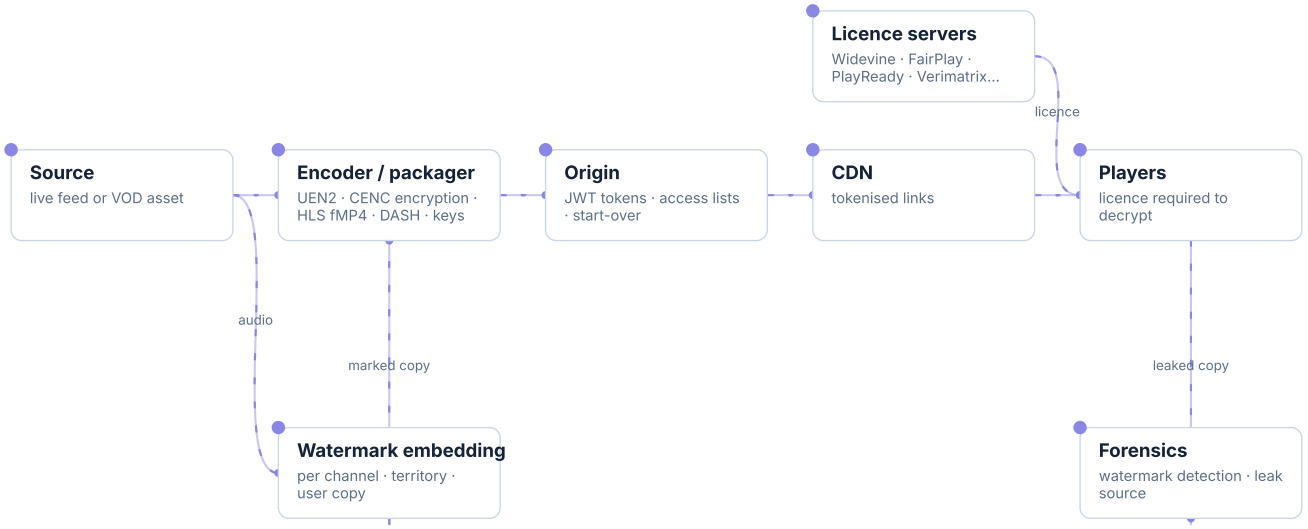
NOISYPEAK SÀRL · EPFL INNOVATION PARK · LAUSANNE · SWITZERLAND · 2026

NOISYPEAK DRM — CONTENT PROTECTION

Noisypeak DRM is the protection stage of the Noisypeak platform. It encrypts HLS and MPEG-DASH output for Apple FairPlay, Google DRM (Widevine, CENC), Microsoft PlayReady, Verimatrix and Nagra PRM, or with an AES-128 static key, directly in the UEN2 encoder and origin. It is for broadcasters and OTT operators who need licensed-device playback on the same pipeline that transcodes and packages their content.

Delivery is controlled at the origin with JWT (RFC 7519) link tokenization, access lists and start-over configured in memory. For content where a leak must be traced, Noisypeak adds forensic audio watermarking: an invisible, encrypted mark per channel, territory or individual viewer that survives re-encoding and camripping, with tools and services to identify the source.

Noisypeak DRM — from source to licensed player



One encrypted packaging feeds every DRM; the origin validates tokens; the watermark lets a leaked copy be traced back.

MULTI-DRM PACKAGING ON THE ENCODER

Encryption is a function of the Noisypeak UEN2 engine, not a separate packager. The same channel that is transcoded is packaged as HLS, HLS3, HLS7 (fMP4) and MPEG-DASH in parallel and encrypted for the DRM systems the audience needs: Apple FairPlay, Google DRM for MPEG-DASH/CENC (Widevine), Microsoft PlayReady, Verimatrix and Nagra PRM. An AES-128 static key is also available. Noisypeak Cell X series encoders ship with DRM in the NPXS-SW licence; the NP-RPK-EMB repack licence includes Google DRM and FairPlay.

- Apple FairPlay · Nagra PRM · Microsoft PlayReady · Verimatrix
- Google DRM for MPEG-DASH / CENC (Widevine)
- AES-128 static key
- HLS · HLS3 · HLS7 fMP4 · MPEG-DASH from one channel

TOKENISED LINKS AND ACCESS CONTROL AT THE ORIGIN

In origin mode the UEN2 node serves the streams itself and validates JWT (RFC 7519) link tokens on every request. Access lists, content protection and start-over are advanced configurations held in memory on the origin. A single origin node is rated for up to 2,500 parallel streams over a 25 Gb/s interface and 20 Gb/s sustained delivery over 25 Gb/s or 2×10 Gb/s LACP interfaces.

- JWT RFC 7519 link tokenization
- Access lists per stream
- Start-over on protected channels
- WebDAV authorization for publishing targets

FORENSIC WATERMARKING

Noisypeak's digital watermarking applies invisible, inaudible encrypted packets to the content so that a copy can later be identified per channel, per territory or down to a specific end-user. It can be applied to an existing content item, to a specific stream, or to an individual user copy during delivery, and can be combined with the transcoding and DRM steps of the Noisypeak Cloud. The mark is not lost when the signal is converted or compressed, and it is robust to copying including camripping.

Compared with usual embedding procedures: generating individual copies takes less time and compute; the secret watermark key is not needed to produce individually marked copies; the unmarked original can be retrieved; and because watermarks are encrypted, unauthorised third parties cannot check for their presence. Noisypeak provides the forensic tools and services to identify the source of a leak.

- Audio watermark, applied in the cloud or on premises
- Granularity: VOD asset · stream · individual user copy
- Content: HLS v2/3 · HLS v5 · DASH · Google Classic DRM (WVM)
- Survives conversion, compression and camripping
- Encrypted mark — undetectable without the key

WATERMARK QUALITY

Audibility was assessed with the commercial OPERA tool implementing the PEAQ model on 180 audio tracks — pop, classical, audio book, interview and camera recordings. The objective difference grade (ODG) scale runs from 0 (inaudible) to −4 (very annoying); the watermarked set scores a median ODG of −1.5.

- OPERA / PEAQ objective difference grades
- 180 test tracks across five content types
- Median ODG −1.5

WHERE IT SITS IN THE PIPELINE

Protection is the stage between enrichment and distribution in the Noisypeak platform: content is captured and transcoded, enriched for FAST and SSAI, protected with DRM, then distributed to B2B2C OTT platforms, set-top boxes, mobile, PC and smart TV. Prism X delivers its ad-stitched HLS/DASH streams with DRM, and Noisypeak Packetizer carries the same origin-mode protection for repacked channels.

FEATURES

Multi-DRM from one encode

FairPlay, Google DRM/CENC (Widevine), PlayReady, Verimatrix and Nagra PRM, encrypted in the UEN2 encoder on the same packaging pass.

AES-128 static key

Static-key encryption of the output without a DRM licence server.

JWT link tokenization

RFC 7519 tokens validated at the origin on every request.

Access lists and start-over

Advanced configurations held in memory on the origin: access lists, content protection, start-over.

Origin throughput

Up to 2,500 parallel streams and 20 Gb/s sustained per node over 25 Gb/s or 2×10 Gb/s LACP.

Forensic watermark

Invisible encrypted marks per channel, territory or user copy; robust to conversion, compression and camripping.

Fast individual copies

Marked copies are generated with less time and compute and without the secret key; the unmarked original can be recovered.

Leak forensics

Tools and services to detect the watermark in a leaked copy and identify its source.

SPECIFICATIONS

DRM SYSTEMS

Apple	FairPlay
Google	Google DRM for MPEG-DASH / CENC (Widevine)
Microsoft	PlayReady
Verimatrix	Supported
Nagra	PRM
Key-only	AES-128 static key

ENCRYPTION AND PACKAGING

Encryption	CENC for MPEG-DASH · FairPlay for HLS · AES-128
Packaging	HLS (TS, separate renditions) · HLS3 (muxed TS) · HLS7 (fMP4) · MPEG-DASH (fMP4), in parallel
Where	Noisypeak UEN2 encoder / origin; NPXS-SW and NP-RPK-EMB licences

TOKENIZATION AND ACCESS

Link tokens	JWT, RFC 7519
Access control	Access lists · content protection · start-over, in-memory configuration
Publishing auth	WebDAV authorization
Origin performance	Up to 2,500 parallel streams over 25 Gb/s · up to 20 Gb/s sustained over 25 Gb/s or 2×10 Gb/s LACP

FORENSIC WATERMARKING

Type	Audio watermark — invisible, inaudible, encrypted
Granularity	Per channel · per territory · per end-user (VOD asset, stream or individual user copy)
Content types	HLS v2/3 (audio muxed in TS) · HLS v5 (separate audio track) · DASH · Google Classic DRM (WVM)
Robustness	Not lost through conversion or compression · robust to copying including camripping
Payload	Encrypted identifying information — channel, territory or user; not detectable by unauthorised parties
Detection	Content owner deciphers the mark; Noisypeak forensic tools and services identify the leak source
Quality	OPERA / PEAQ, 180 tracks · median ODG −1.5
Deployment	Noisypeak Cloud or on premises; with or without Noisypeak transcoding and DRM steps

MODELS AND LICENCES

NPXS-SW

Noisypeak Cell software licence — MPEG2 / H.264 / HEVC / AV1, HLS/DASH packetizing, WebDAV, DRM, SCTE-35

NP-RPK-EMB

Noisypeak Repack licence — HLS/DASH out with Google DRM and FairPlay support, for integrated solutions

WHERE IT IS USED

Premium live channels on OTT

One encrypted HLS/DASH packaging plays through FairPlay, Widevine or PlayReady on the viewer's device.

Operator platforms with Verimatrix or Nagra

Operators keep their existing Verimatrix or Nagra PRM protection on the Noisypeak encoding pipeline.

Token-gated catch-up and start-over

JWT links and access lists control who can open a protected stream at the origin.

Tracing a leak

Per-user watermarked copies identify the account behind a pirated stream, even after camripping.

Noisypeak Sàrl
EPFL Innovation Park, Bâtiment D
CH-1015 Lausanne, Switzerland
CHE-270.718.196

Sales and evaluation
sales@noisypeak.com
+41 22 575 37 57
noisypeak.com

Works with
Noisypeak Cell · Noisypeak Packetizer · Prism X

Noisypeak, Noisypeak Connected and Noisypeak DigitalEye are service marks and trademarks of Noisypeak. All other trademarks, service marks, trade names, product names and logos are the property of their respective owners. Specifications are subject to change without notice. © 2026 Noisypeak Sàrl. All rights reserved.