# Digital Rights Management ( DRM )

Carmen Salinas - TCC

# Presentación

- Panorama General
- Encripción
- Widevine
- Fairplay

# Panorama General

# Tipos

## Widevine

- Implementado por Google.
- Para formato contenedor MP4 sobre DASH.
- Utiliza encripción basada en CTR.

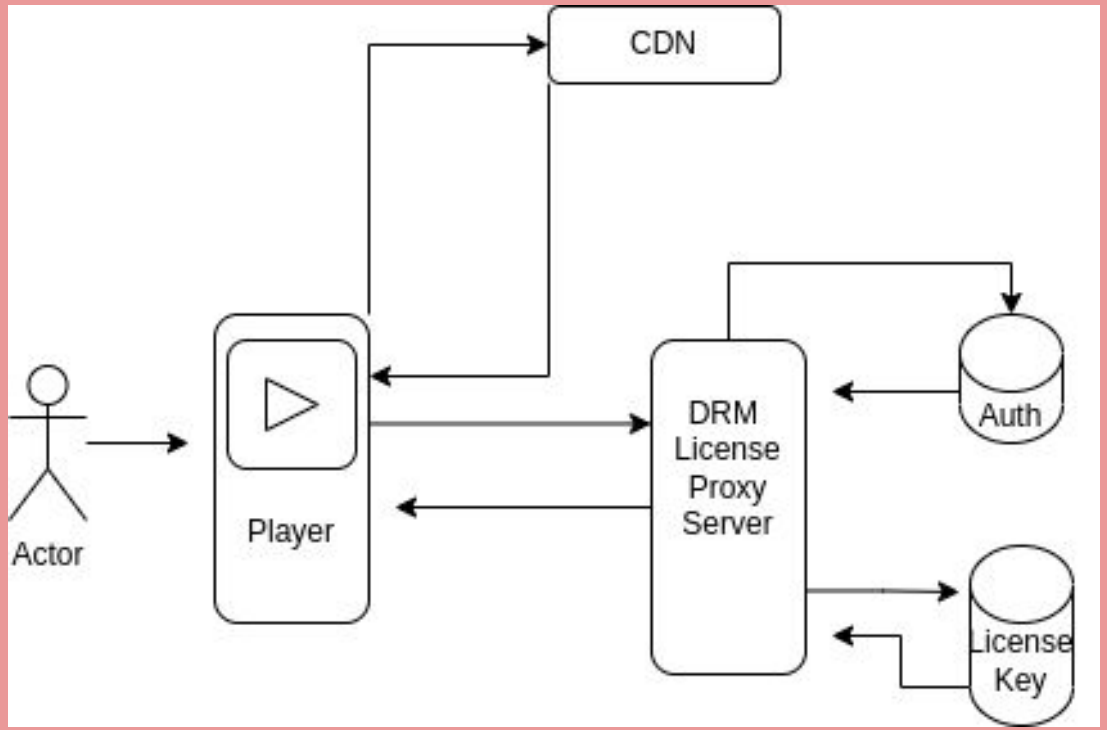
## Fairplay

- Desarrollado por Apple.
- Para formato contenedor TS y MP4 sobre HLS.
- Utiliza encripción CBC.

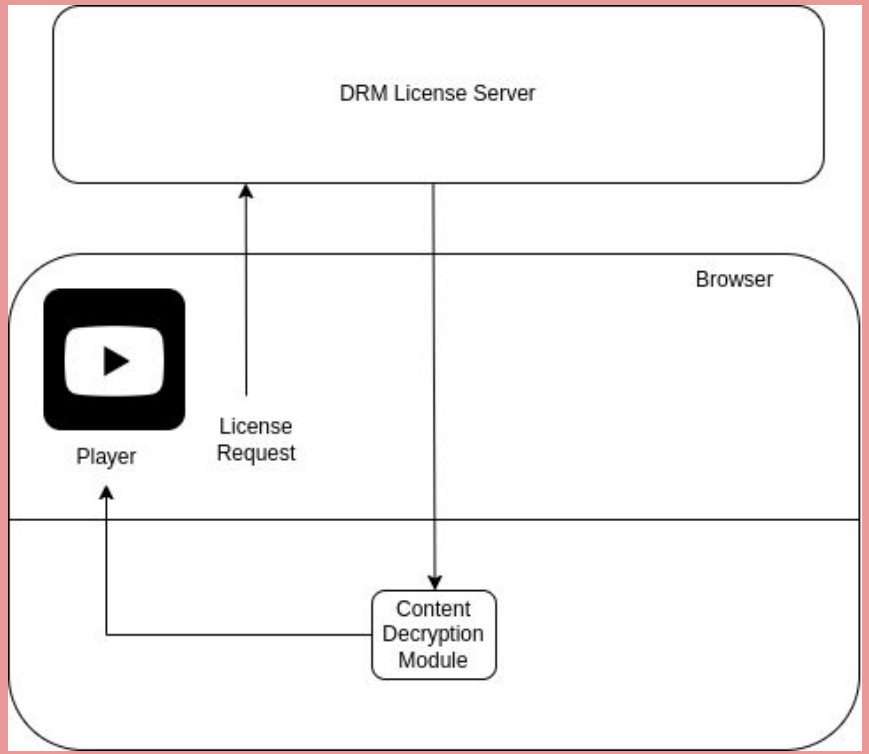
## PlayReady

- Desarrollado por Microsoft.

# Funcionamiento

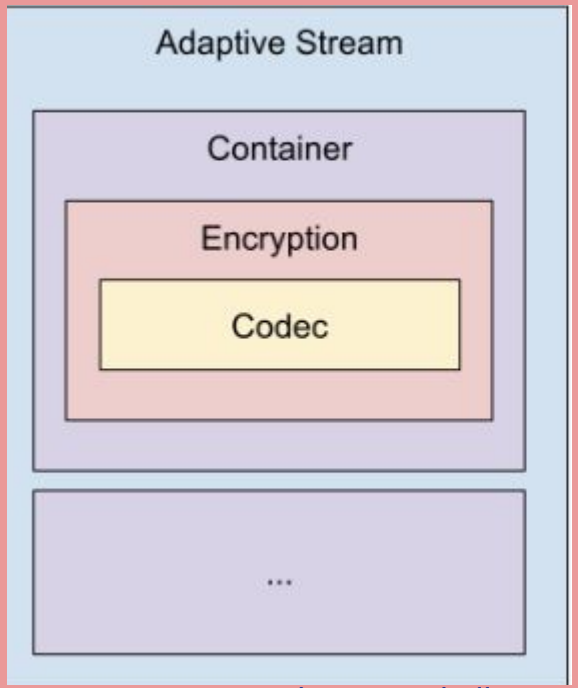


# Funcionamiento

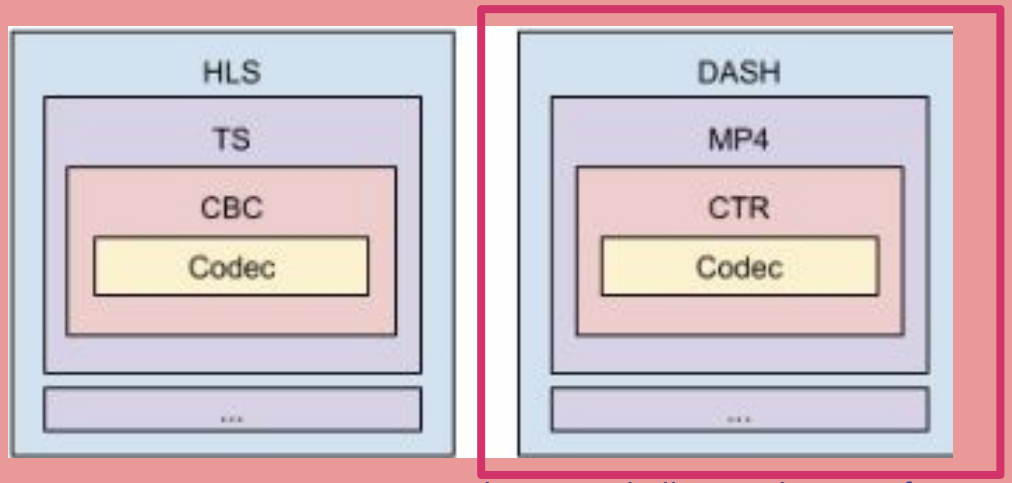


# Encripción

- Advanced Encryption Standar (AES)
  - Basado en criptografía simétrica.
  - Widevine y Fairplay usan claves de 128 bits y un vector inicial (IV).
- Se definen en **CENC** dos modos de encripción:
  - **CTR** -> AES Counter Mode
  - **CBC** -> AES Cipher-Block

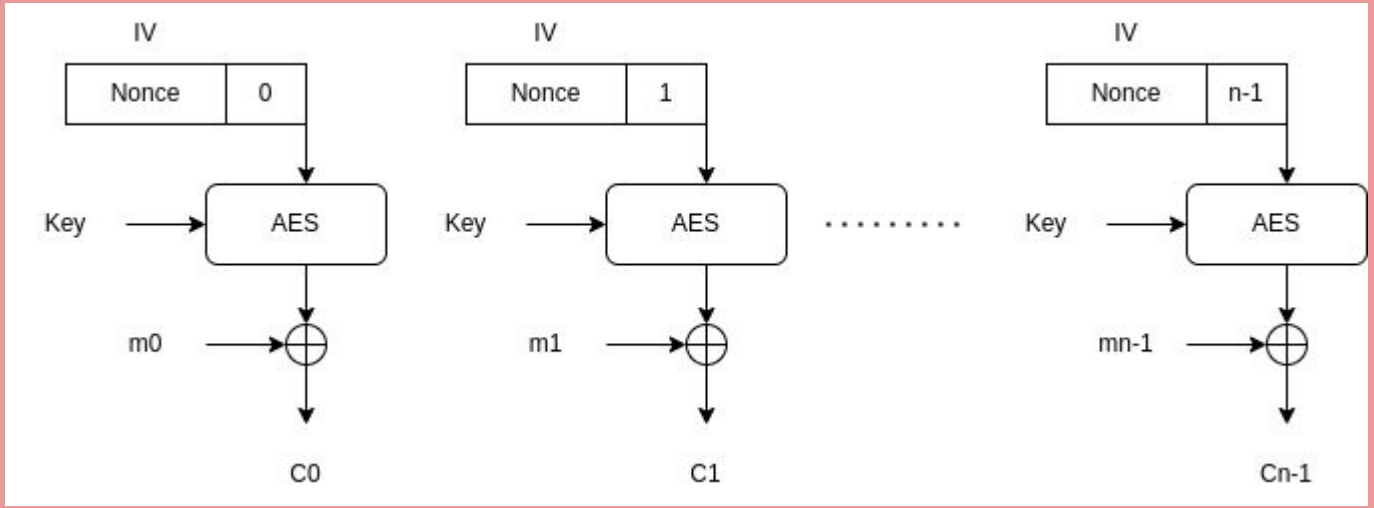



CBCS versus CMAF versus TS : https://ottball.com/cbcs-cmaf-ts/




CBCS versus CMAF versus TS : https://ottball.com/cbcs-cmaf-ts/

# CTR

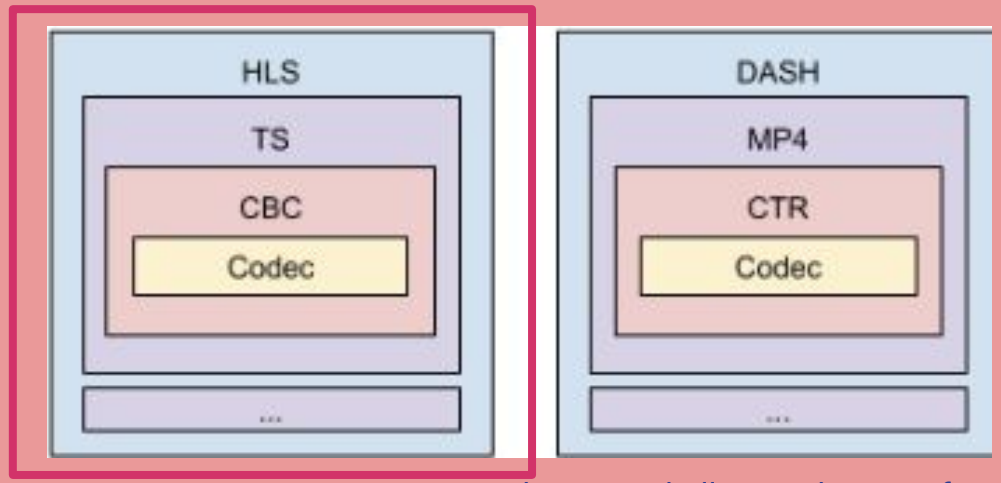



Encripción

$$C_i = E_k(nonce||i) \oplus m_i$$

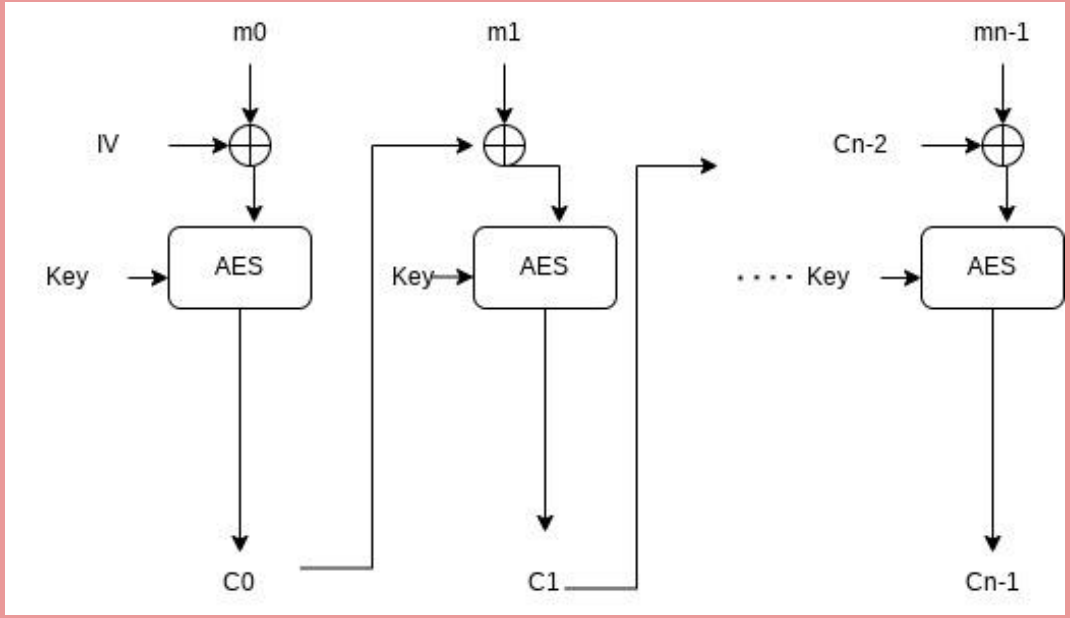
Desencripción

$$m_i = c_i \oplus E_k(nonce||i)$$




CBCS versus CMAF versus TS : https://ottball.com/cbcs-cmaf-ts/

# CBC

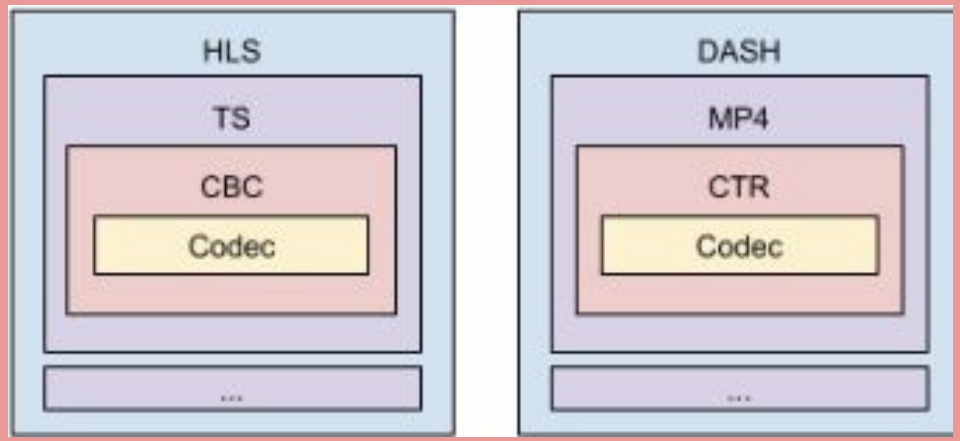



Encripción

$$C_i = E_k(m_i \oplus C_{i-1})$$

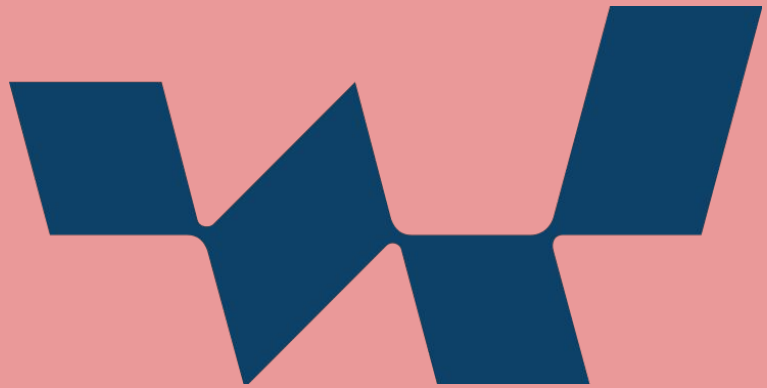
Desencripción

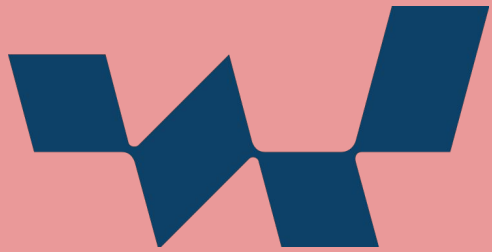
$$m_i = E_k(C_i) \oplus C_{i-1}$$




CBCS versus CMAF versus TS : https://ottball.com/cbcs-cmaf-ts/

# Widevine



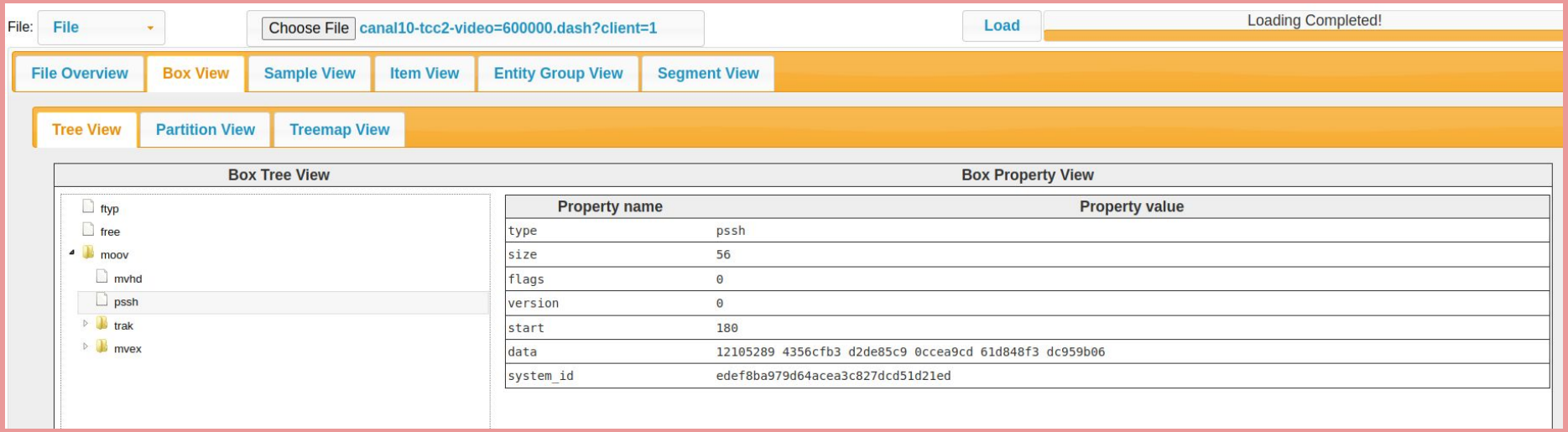


- Desarrollado por Google.
- Para formato contenedor MP4 sobre DASH.
- Dos maneras de implementarlo:
  - Solución de Google.
  - Implementación propia.
- Encripción basada en CTR.
- Utilizado en TCC,Netflix, HBO MAX, entre otros.

# ¿Cómo saber que el contenido está encriptado?

```
<!-- Common Encryption -->
<ContentProtection
  schemeIdUri="urn:mpeg:dash:mp4protection:2011"
  value="cenc"
  cenc:default_KID="52894356-CFB3-D2DE-85C9-0CCEA9CD61D8">
</ContentProtection>
<!-- Widevine -->
<ContentProtection
  schemeIdUri="urn:uuid:EDEF8BA9-79D6-4ACE-A3C8-27DCD51D21ED">
</ContentProtection>
```

# ¿Cómo saber que el contenido está encriptado?



FairPlay

FairPlay

# FairPlay

- Desarrollado por Apple.
- Se aplica a TS sobre HLS.
- Encripción basada en CBC.
- Utilizado en TCC, Netflix, HBO MAX, entre otros.

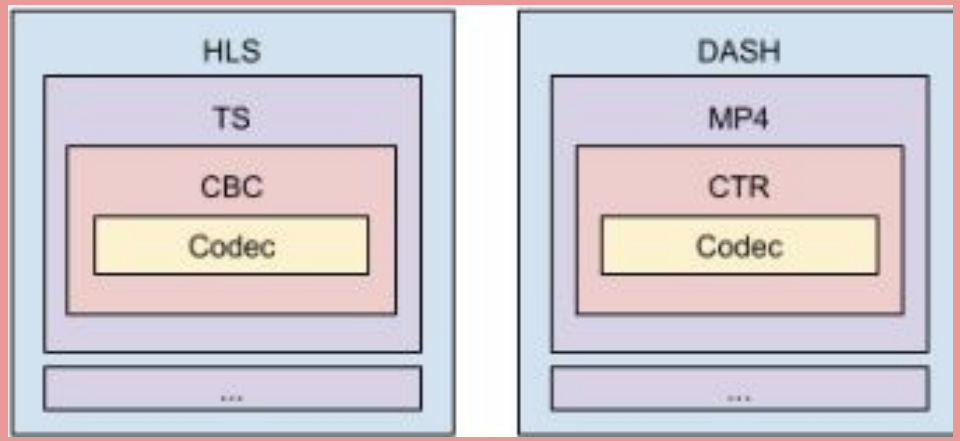
FairPlay

¿Cómo saber que el contenido está encriptado?

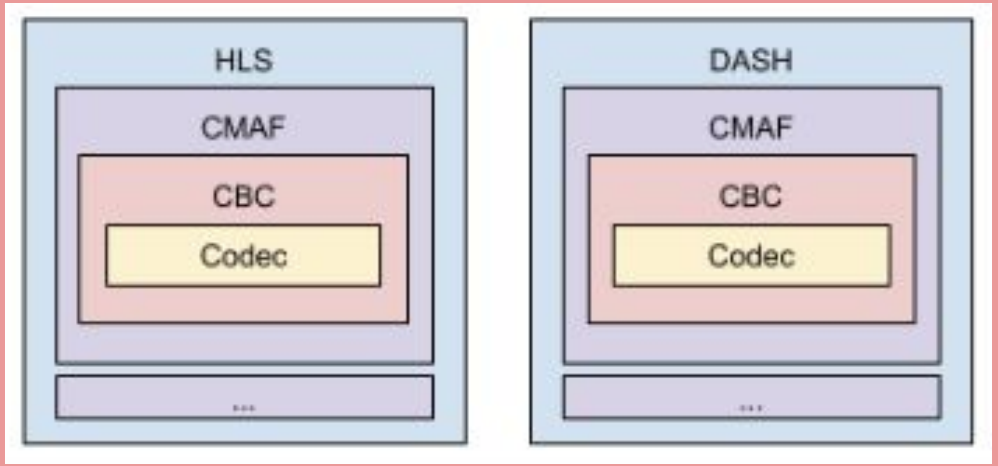
```
#EXTM3U
#EXT-X-VERSION:5
#EXT-X-TARGETDURATION:10
#EXT-X-MEDIA-SEQUENCE:0
#EXT-X-KEY:METHOD=SAMPLE-AES,URI="skd://7oxpcY1PgPuvhXHuyDuUoA==?wowzasessionid=1599088807",KEYFORMAT="com.apple.streamingkeydelivery",KEYFORMATVERSIONS="1"
#EXTINF:10,
media_w1599088807_b1200000_0.ts
#EXTINF:10,
media_w1599088807_b1200000_1.ts
#EXTINF:10,
media_w1599088807_b1200000_2.ts
#EXTINF:10,
media_w1599088807_b1200000_3.ts
#EXTINF:10,
media_w1599088807_b1200000_4.ts
#EXTINF:10,
media_w1599088807_b1200000_5.ts
#EXTINF:10,
media_w1599088807_b1200000_6.ts
#EXTINF:10,
media_w1599088807_b1200000_7.ts
#EXTINF:10,
media_w1599088807_b1200000_8.ts
#EXTINF:10,
media_w1599088807_b1200000_9.ts
#EXTINF:10,
media_w1599088807_b1200000_10.ts
#EXTINF:10,
media_w1599088807_b1200000_11.ts
#EXT-X-ENDLIST

```

# ¿Qué va a pasar en el futuro?




CBCS versus CMAF versus TS : https://ottball.com/cbcs-cmaf-ts/




CBCS versus CMAF versus TS : https://ottball.com/cbcs-cmaf-ts/

# Fin :)