Digital Rights Management Demystified

Common Issues and Solutions

Johannes Jauch, *CTO, Axinom*

Pieter-Jan Speelmans, *CTO, THEO Technologies*

axinom!

THEO

axinom!

Johannes Jauch

CTO, Axinom

As the leader of the technology team, Johannes is responsible for defining the technological trail Axinom blazes.

He works to empower organizations in understanding and leveraging Axinom products and solutions to solve real-world issues such as content piracy, revenue protection, scalability of services, and much more.

THEO

Pieter-Jan Speelmans

CTO, THEO Technologies

Pieter-Jan is the Founder and the head of the technical team at THEO Technologies. He is the brain behind THEOplayer, HESP and EMSS.

With a mission to 'Make Streaming Video Better Than Broadcast', he is innovating the way video is delivered online from playback all the way to ultra-low latency streaming. Pieter-Jan is committed to enable media companies to easily offer exceptional video experience across any device.

1.

Adhering to the requirements of content owners.

How to implement different keys and configurations for different stream qualities?

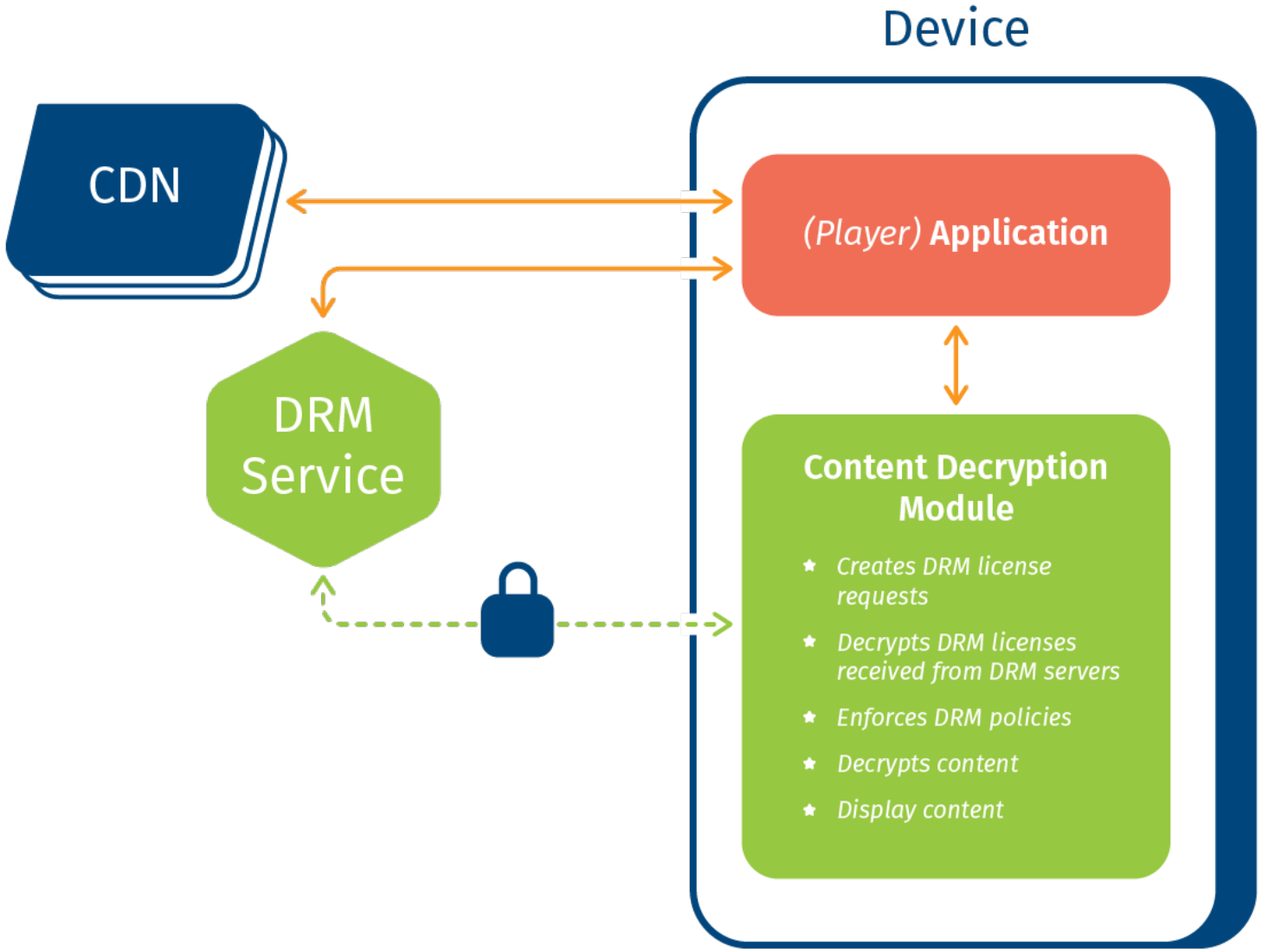
axinom! THEO

A typical requirement from a content owner

- Audio, SD, and HD tracks must use separate encryption keys.
- Hardware-backed DRM is mandatory for resolutions of 1080p and above.
- When video is displayed on an external screen the system must enforce the use of the HDCP protocol version 2.2 or above.
- In any case video display on external screens must be prevented for resolutions of 1080p and above.

axinom! THEO

Why encrypt with multiple keys?



axinom! THEO

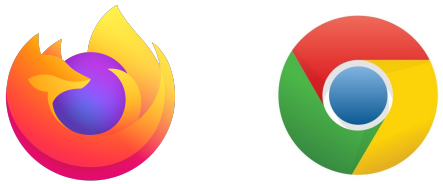
Content Decryption Module flavors

Hardware-backed:

Widevine Security Level 1

PlayReady Security Level 3000

Purely software:



Widevine Security Level 3

PlayReady Security Level 2000

axinom! THEO

Why encrypt with multiple keys?

Content owners want flexibility

A sample use case:

- Provide HD/UHD or HDR content only to clients with hardware-backed DRM
- Reach the broadest audience by providing content in lower resolutions to as many devices as possible

Solution:

- Use different encryption keys for encrypting different tracks in ABR assets
- Authorize devices based on their capabilities

axinom! THEO

Sample Asset

Sample MPEG-DASH asset		
Representation	Resolution	Encryption key
Audio	-	Key 1
Video	480p	Key 2
Video	640p	Key 2
Video	720p	Key 3
Video	1080p	Key 3
Video	2160p	Key 4

axinom! THEO

But wait..can‘t I just keep two versions, each encrypted with just one key?

axinom! THEO

How to achieve multi-key encryption end-to-end?

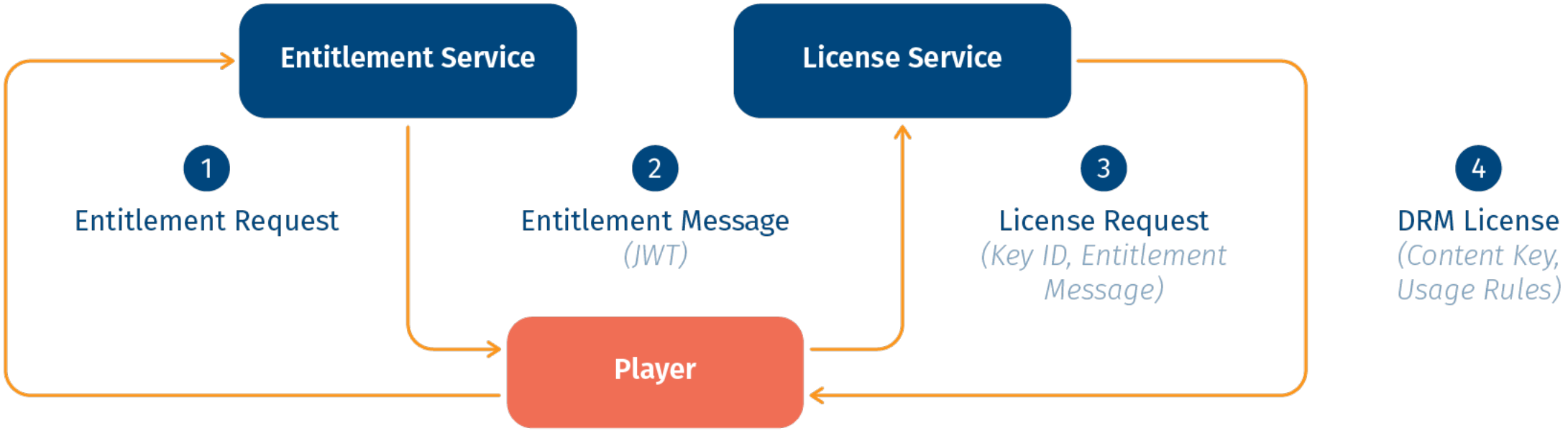
Components in the delivery chain that need to support multi-key assets:

- The encoder/packager
- The DRM key service
- The DRM license service
- The player

Axinom and THEOplayer have you covered.

axinom! THEO

Authorizing playback at runtime



JWT – *JSON Web Token* is a widely supported standard

axinom! THEO

Contents of an Entitlement Message (represented as JWT)

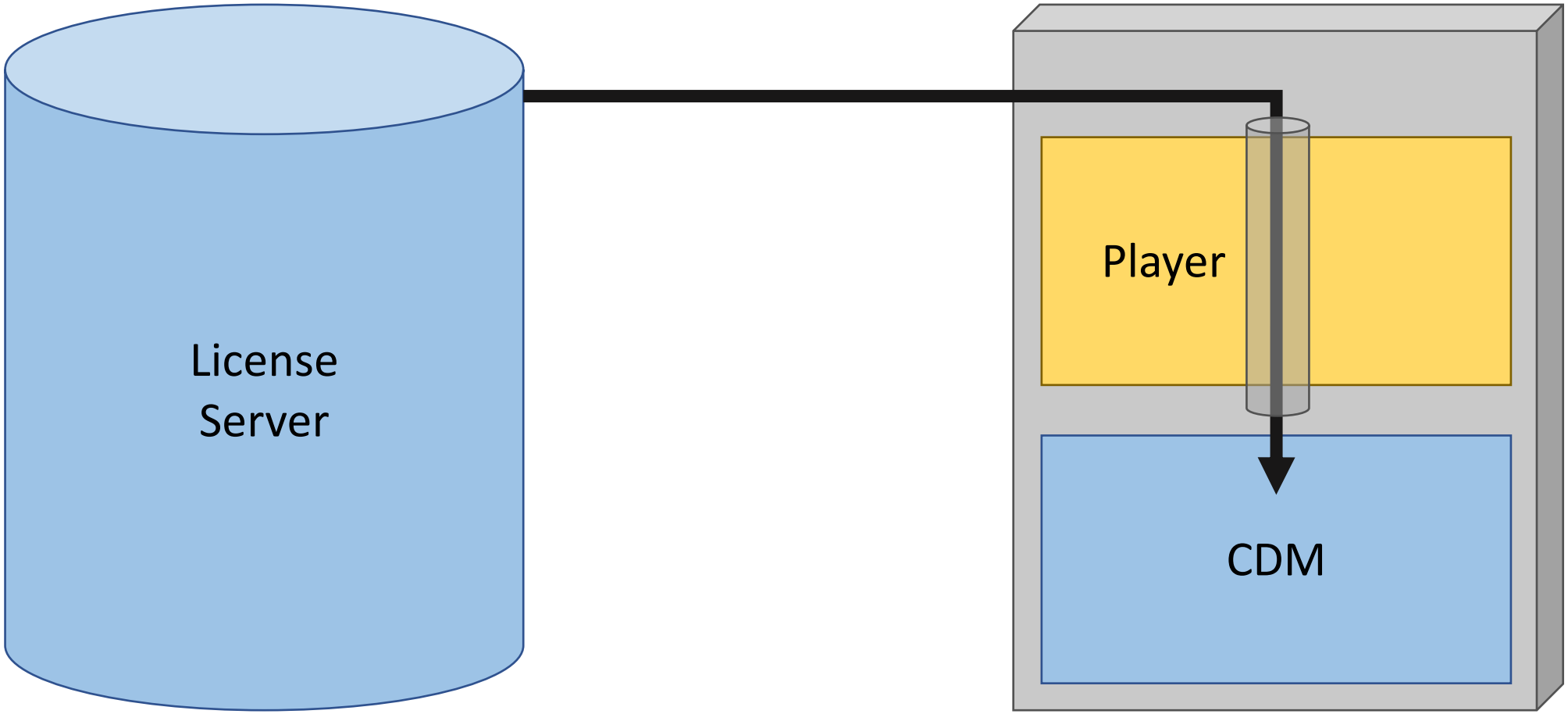
```
...
"content_keys_source": {
    "inline": [
        {
          "id": ”c39ad9e7-0ab3-4534-9e9f-9853615e26f6",
          "usage_policy": "Audio"
        },
        {
          "id": ”6d329dff-db5e-48ef-b096-3ef347b16c7f",
          "usage_policy": "SD"
        },
        {
          "id": "29f05e8f-a1ae-46e4-80e9-22dcd44cd7a1",
          "usage_policy": "HD"
        }
    ]
  },
"content_key_usage_policies": [
    {
      "name": "Audio”
    },
    {
      "name": "SD",
      "widevine": {
        "device_security_level": "SW_SECURE_CRYPTO",
        "hdcp": "2.2"
      },
      "playready": {
        "min_device_security_level": 2000,
        "uncompressed_digital_video_opl": 300
      }
    },
    {
      "name": "HD",
      "widevine": {
        "device_security_level": "HW_SECURE_ALL",
        "hdcp": "NO_DIGITAL_OUTPUT"
      },
      "playready": {
        "min_device_security_level": 3000,
        "uncompressed_digital_video_opl": 400
      }
    }
  ]
}
```

axinom! THEO

What about the player side?

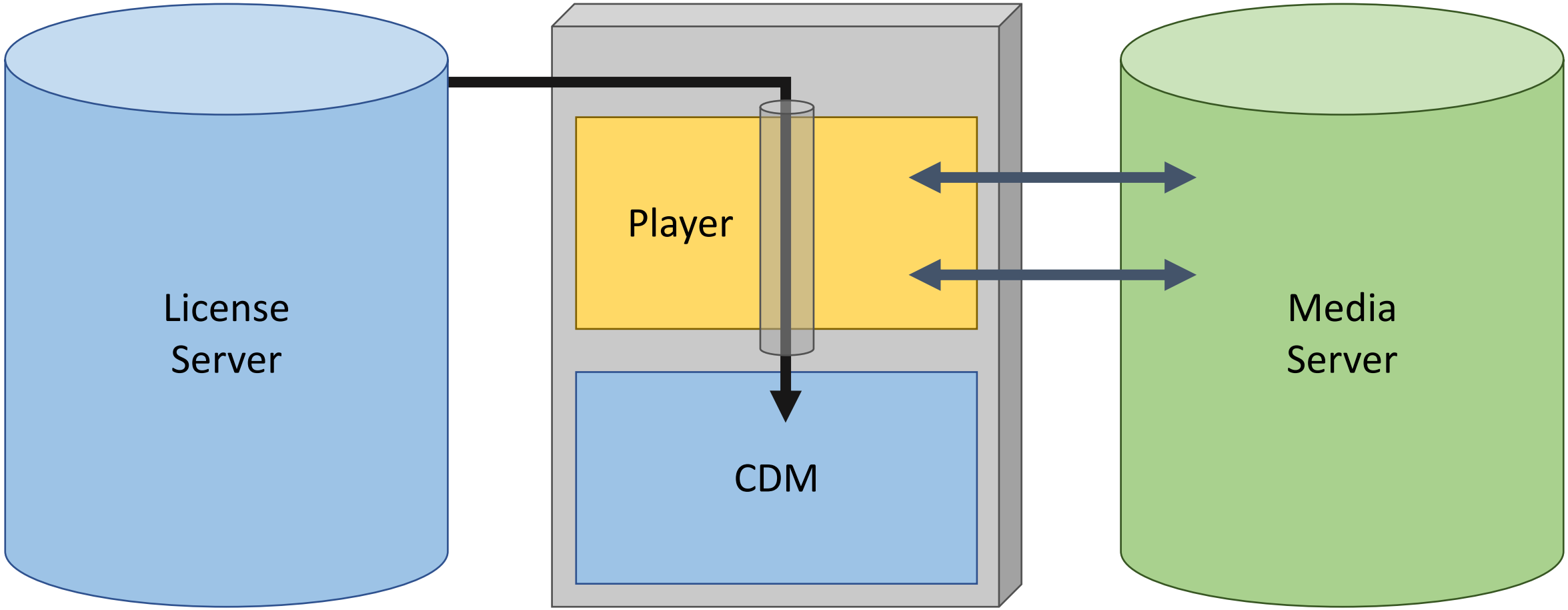
axinom! THEO

What about the player side?



axinom! THEO

What about the player side?



axinom! THEO

Thou shalt not stall

axinom! THEO

An unaware player's approach to quality switching

Step 1: Determine which stream to switch to

Step 2: (Optionally download an updated playlist or manifest.)

Step 3: (Optionally download a map or initializer file & append it to the buffer.)

Step 4: Download the media data & append it to the buffer.

Step 5: Play

axinom! THEO

An unaware player's approach to quality switching

Step 1: Determine which stream to switch to

Step 2: (Optionally download an updated playlist or manifest.)

Step 3: (Optionally download a map or initializer file & append it to the buffer.)
Optionally a license request

Step 4: Download the media data & append it to the buffer.
Optionally a license request

Step 5: Play

axinom! THEO

An unaware player's approach to quality switching

Step 1: Determine which stream to switch to

Step 2: (Optionally download an updated playlist or manifest.)

Step 3: (Optionally download a map or initializer file & append it to the buffer.)
Optionally a license request

Step 4: Download the media data & append it to the buffer.
Optionally a license request

Step 4b: Issue a license request and pass the response to the CDM.

Step 5: Play

axinom! THEO

Thou shalt not stall

axinom! THEO

An unaware player's approach to quality switching

Step 1: Determine which stream to switch to
and identify if another key is needed

Step 2: (Optionally download an updated playlist or manifest.)

Step 3: (Optionally download a map or initializer file & append it to the buffer.)

Step 4: Download the media data & append it to the buffer.

Step 5: Play

axinom! THEO

An unaware player's approach to quality switching

Step 1: Determine which stream to switch to
and identify if another key is needed

Step 2: (Optionally download an updated playlist or manifest.)
identify the PSSH and use it to do an early request for the license

Step 3: (Optionally download a map or initializer file & append it to the buffer.)

Step 4: Download the media data & append it to the buffer.

Step 5: Play

axinom! THEO

An unaware player's approach to quality switching

Step 1: Determine which stream to switch to
and identify if another key is needed
and decide if you will really want to make the switch, and have the buffer to do this

Step 2: (Optionally download an updated playlist or manifest.)
identify the PSSH and use it to do an early request for the license

Step 3: (Optionally download a map or initializer file & append it to the buffer.)

Step 4: Download the media data & append it to the buffer.

Step 5: Play

axinom! THEO

An aware player’s approach to quality switching

Step 0: Ensure your CDM is set up to handle the most strict restrictions (if possible).

Step 1: Determine which stream to switch to
and identify if another key is needed
and decide if you will really want to make the switch, and have the buffer to do this

Step 2: (Optionally download an updated playlist or manifest.)
identify the PSSH and use it to do an early request for the license

Step 3: (Optionally download a map or initializer file & append it to the buffer.)

Step 4: Download the media data & append it to the buffer.

Step 5: Play

2.

Why is protecting live/linear streaming so hard?

axinom! THEO

Scenario 2: Protecting linear streaming

Content owner:

“Linear streams must rotate encryption keys every 2 hours.”

axinom! THEO

Scenario 2: Protecting linear streaming

Naive approach

- Announce a new <Period> when keys must rotate. Let end user devices find out and send license requests.

axinom! THEO

axinom! THEO

Scenario 2: Protecting linear streaming

Let‘s do some math:

Audience: 1 million

Latency ~30 seconds

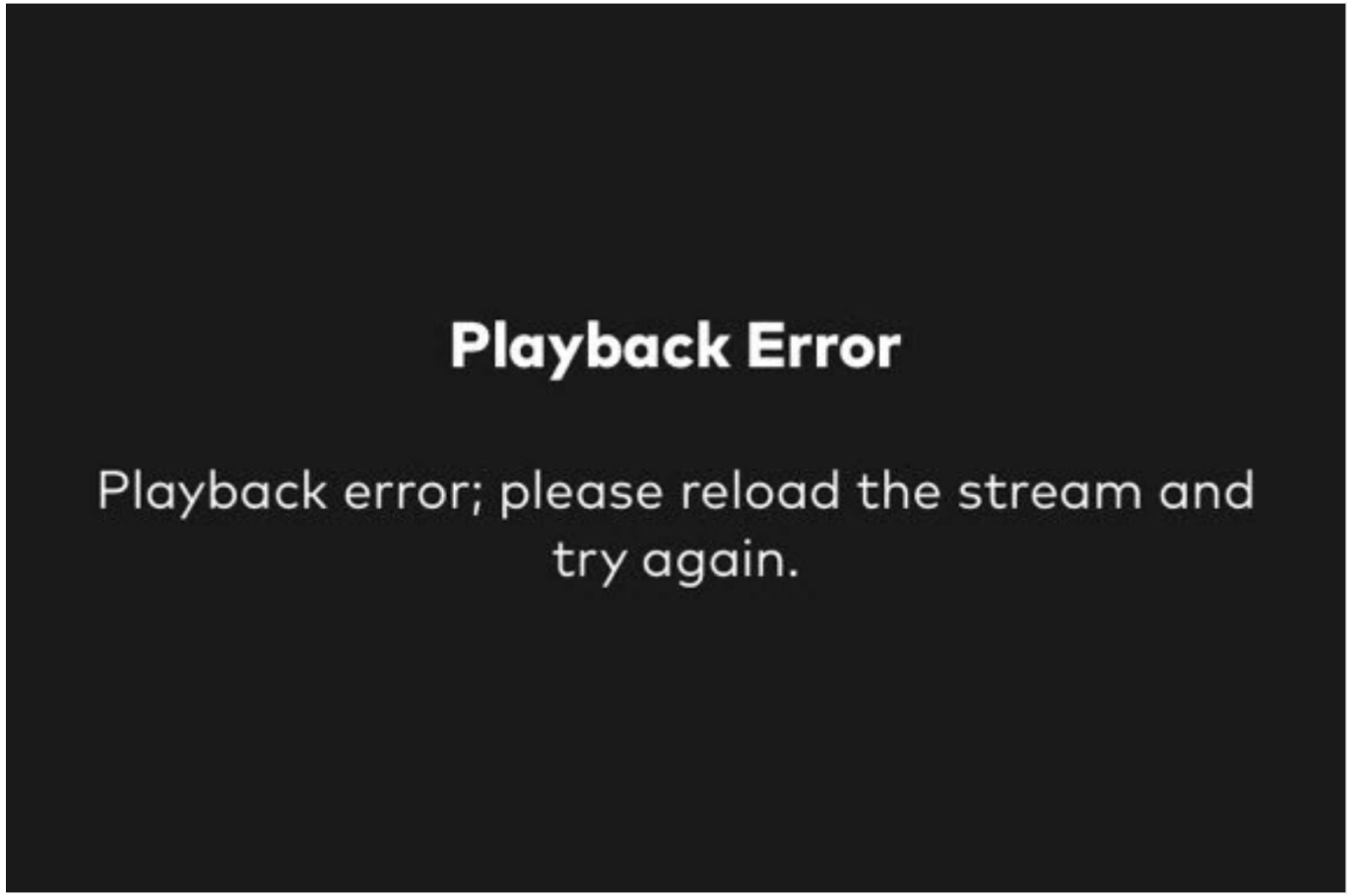
axinom! THEO

Scenario 2: Protecting linear streaming

>30.000 rps

axinom! THEO

Scenario 2: Protecting linear streaming



axinom! THEO

Scenario 2: Protecting linear streaming

Mitigation strategies:

- Increase service capacity
- Distribute license acquisition over time

axinom! THEO

Scenario 2: Protecting linear streaming

Live events – when stretching over time is NOT possible:

- A (potentially) large audience tunes in at the very same time
- Everyone needs a license NOW.

axinom! THEO

Scenario 2: Protecting linear streaming

Have a big audience? When working with a DRM service vendor verify that

- Your capacity needs can be met (with some margin)
- In the geography of your expected audience
- Test it

axinom! THEO

Scenario 2: Protecting linear streaming

Wait a minute.

- Does the multi-key topic have any impact on this?

axinom! THEO

Spread the  !

Spreading the load

500.000 rps

axinom! THEO

Spreading the load

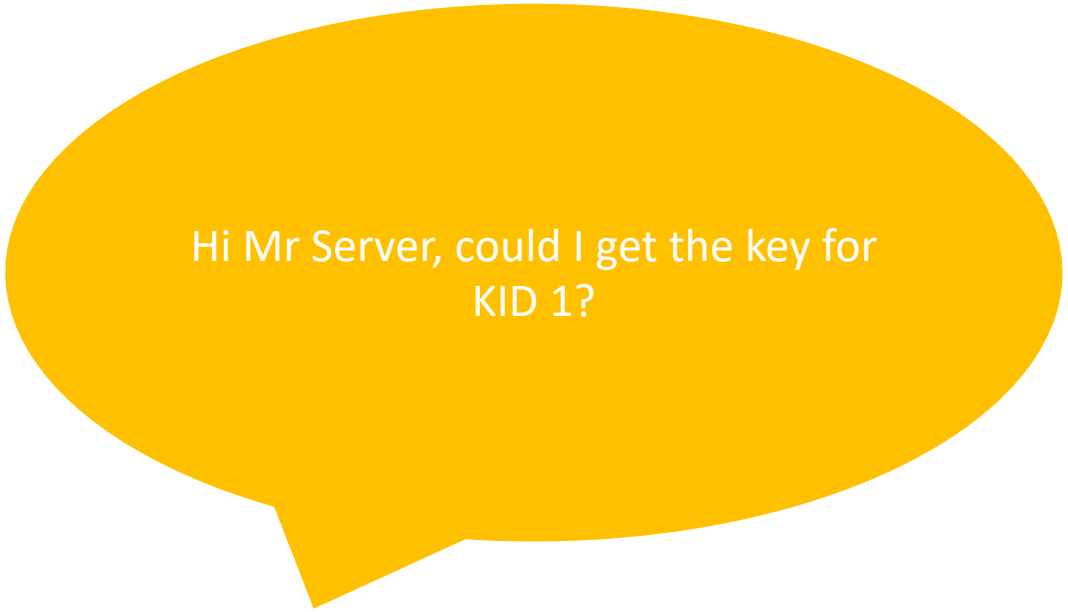
500.000 rps

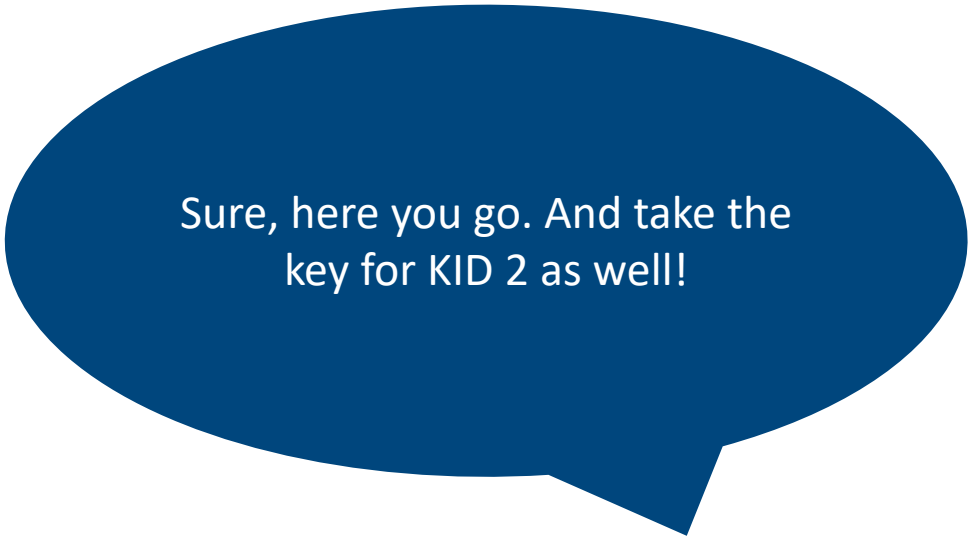
for 2s, then nothing...

axinom! THEO

axinom! THEO

How about using multiple keys in one license?


Hi Mr Server, could I get the key for KID 1?


Sure, here you go. And take the key for KID 2 as well!

But this just delays the problem...

axinom! THEO

But this just delays the problem...

Not really, a smart player can handle this

3.

Integrating DRM in your content supply chain.

How to get started with DRM implementation?

https://portal.axinom.com

Get started now!

Visit:

axinom.com/drm

theoplayer.com