PallyCon 라이선스 콜백 가이드 v1.0

개요 {#intro}

PallyCon 클라우드 서버에서 멀티 DRM(FPS, Widevine, PlayReady, NCG) 라이선스를 발급하는 방식은 콜백 방식과 토큰 방식이 있습니다.

1. 콜백 방식

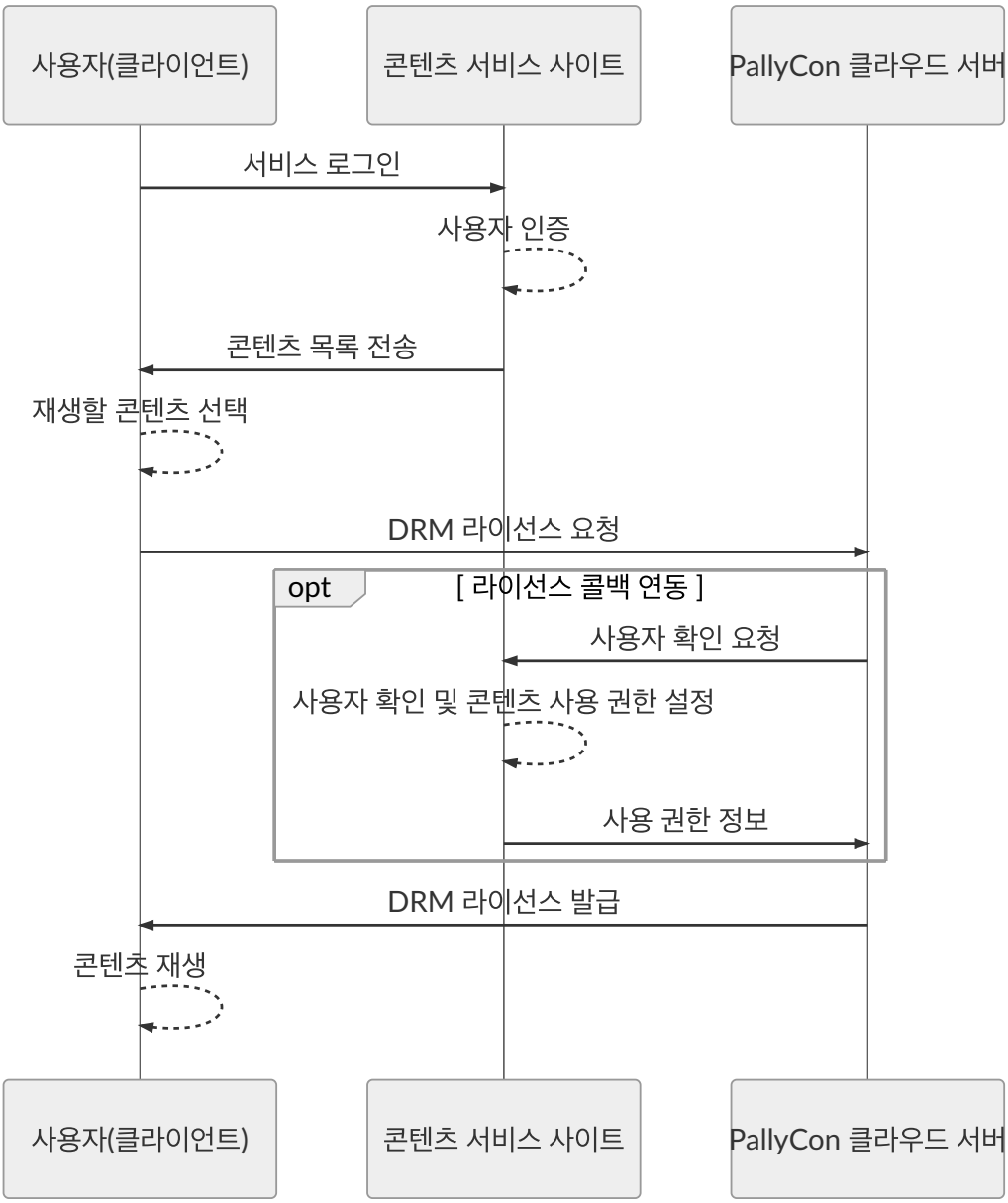
- PallyCon 클라우드 서버는 멀티 DRM 클라이언트로부터 라이선스 요청을 받으면 먼저 해당 사용자가 유효한 권한이 있는지 해당 서비스 사이트의 콜백 페이지를 통해 확인합니다.
- 권한이 있는 사용자로부터의 요청인 경우, 서비스 사이트는 콜백 웹 페이지를 통해 인증 여부, 사용 권한(무제한, 기간제), 각종 보안 옵션 등의 정보를 PallyCon 클라우드 서버에게 리턴합니다.
- PallyCon 클라우드 서버는 콜백 페이지의 응답을 받아 클라이언트에 해당 라이선스를 발급합니다.

2. 토큰 방식

- 멀티 DRM 클라이언트에서 콘텐츠 재생 시, 서비스 사이트는 미리 정의된 규격에 따라 라이선스 토큰을 생성해 전달할 수 있습니다.
- 서비스 사이트는 토큰 생성 규격을 통해 사용 권한(무제한, 기간제)과 각종 보안 옵션 등을 설정할 수 있습니다.
- 클라이언트가 토큰과 함께 라이선스를 요청하면, PallyCon 클라우드 서버는 해당 토큰의 유효성을 확인한 후 라이선스를 발급합니다.

본 문서는 첫 번째 방식인 콜백 방식의 API에 대해 설명합니다. 토큰 방식에 대한 상세 규격은 라이선스 토큰 가이드를 참고하시기 바랍니다.

라이선스 발급 과정 {#workflow}



1. 콘텐츠 재생 준비

- 클라이언트(Player)에서 DRM 콘텐츠 재생을 위해 서비스 사이트로부터 DRM 연동을 위한 정보(PallyCon Custom Data)를 전달받아 DRM 콘텐츠 재생을 시도합니다.
- NCG DRM 콘텐츠를 재생하는 경우에는 Custom Data 전달 과정이 생략됩니다.

2. 라이선스 요청

- 플레이어는 재생에 필요한 DRM 라이선스를 PallyCon 클라우드 서버에 요청합니다.

3. 콜백 사용자 인증 (아래 규격 참조)

- PallyCon 클라우드 서버는 해당 서비스 사이트에 사용자 인증 요청을 합니다.

4. 사용 권한 정보 응답

- 서비스 사이트의 라이선스 콜백 페이지에서 사용자 인증 확인 후 콘텐츠 사용 권한 정보를 회신합니다.

5. 라이선스 발급

- PallyCon 클라우드 서버는 콜백 페이지로부터 받은 권한 정보를 해당 DRM 유형(FPS, Widevine, PlayReady and NCG)에 맞는 라이선스로 생성해 발급합니다.

라이선스 콜백 API (JSON 방식) {#callback-json}

요청 데이터 규격

- Request URI : PallyCon 콘솔 사이트의 '콘텐츠 사용 정보 URL' 세팅에 등록된 URL로 요청됩니다.
- Request Method : POST
- Character set : UTF-8
- POST body : request parameters

Key	Value
data	base64 Encoding (aes256 Encrypt (**JSON Data string**))

> [AES256 암호화 항목](#) 참조

JSON 요청 데이터 형식

```
{
    "user_id": "<User ID>",
    "cid": "<Content ID>",
    "oid": "<Optional ID>",
    "nonce": "<Random String>",
    "device_id": "<Device ID>",
    "device_type": "<Device Type>",
    "drm_type": "<DRM Type>"
}
```

Name	Value	Required	Description
user_id	string	Yes	서비스 사이트 사용자 ID

Name	Value	Required	Description
cid	string	Yes	재생하려는 콘텐츠의 ID. 최대 200 바이트 영숫자
oid	string	No	부가 연동 정보. 주문 정보 등 추가적으로 서비스 사이트에 전달되기를 원하는 정보를 입력합니다. 사용 여부는 선택 사항입니다.
nonce	string	Yes	One time Random String. 응답을 보낼 때 동일 값으로 회신해야 합니다.
device_id	string	No	클라이언트 기기의 ID (NCG DRM에만 해당)
device_type	string	No	기기 유형(NCG DRM에만 해당) OS-X, Windows, Android, iOS
drm_type	string	Yes	DRM 유형 (“NCG”, “Widevine”, “PlayReady”, “FairPlay”)

응답 데이터 규격

- body : base64 Encoding (aes256 Encrypt (**JSON Data string**))

JSON 응답 데이터 형식

```
{
    "error_code": "<Error Code>",
    "error_message": "<Error Message>",
    "response_user_id":"<response user id>",
    "playback_policy": {
    "limit": <true|false>,
    "persistent": <true|false>,
    "duration" : <int(seconds)>,
    "expire_date": "<yyyy-mm-ddThh:mm:ssZ>"
    },
    "security_policy": {
        "hardware_drm": <true|false>,
        "output_protect": {
            "allow_external_display" : <true|false>,
            "control_hdcp": <0|1|2>
        },
        "allow_mobile_abnormal_device" : <true|false>,
        "playready_security_level" : <150|2000>
```

```
    },
    "external_key": {
        "mpeg_cenc": {
            "key_id" : "<hex-string>",
            "key" : "<hex-string>",
            "iv" : "<hex-string>"
        },
        "hls_aes" : {
            "key" : "<hex-string>",
            "iv" : "<hex-string>"
        },
        "ncg":{
            "cek":"<hex-string>"
        }
    },
    "nonce": "<Random String>"
}
```

Name	Value	Required	Description
error_code	string	Yes	"0000" : 성공, 에러인 경우 서비스 업체에서 정의된 숫자로 된 에러 코드
error_message	string	Yes	에러인 경우 에러 메시지
response_user_id	string	No	license 요청에 포함된 user ID를 콜백 페이지에서 응답한 별도 ID로 변경합니다. 클라이언트에서 해당 서비스의 user ID 정보를 알 수 없는 경우에 사용합니다. (선택 사항)
playback_policy	json	Yes	재생 관련 룰 설정 (상세 규격 참조)
security_policy	json	No	보안 관련 룰 설정 (상세 규격 참조)
external_key	json	No	키 정보를 PallyCon 클라우드에서 관리하지 않고 별도로 패키징한 콘텐츠에 외부 키 정보를 입력하여 라이선스 요청 시 사용. (상세 규격 참조)
nonce	string	Yes	One time Random String. 요청에 포함된 것과 동일한 값으로 회신합니다.

playback_policy {#playback-policy}

Name	Value	Required	Description

Name	Value	Required	Description
limit	boolean	No	기간제 적용 여부 (기본값: false) true : 기간제, false : 무제한
persistent	boolean	No	오프라인용 라이선스 저장 여부. (기본값: false) true : 라이선스 유지, false : 재생 후 라이선스 제거(스트리밍)
duration	number	Select	라이선스 유효 기간 (단위 : 초). **duration, expire_date 동시 설정 시, duration 값이 우선됩니다.** 'limit'값이 true인 경우에만 적용됩니다. (false일 경우 이 항목은 무시)
expire_date	string	Select	라이선스 만료 날짜, GMT Time 표기'yyyy-mm-ddThh:mm:ssZ' 'limit'값이 true인 경우에만 적용됩니다. (false일 경우 이 항목은 무시) duration 항목과 함께 사용 시, 이 값은 무시됩니다.

security_policy (optional) {#security-policy}

Name	Value	Required	Description
hardware_drm	boolean	No	하드웨어 DRM 적용 여부. (기본값 false) - 각 DRM 종류에 따라 security level 설정 - cenc(widevine modular) 컨텐츠에만 적용됨
output_protect	json	No	외부 출력 룰 설정 (상세 규격 참조)
allow_mobile_abnormal_device	boolean	No	탈옥 기기 재생 허용 여부 (기본값 false)
playready_security_level	number	No	PlayReady 보안 레벨 설정, 150,2000 (기본값 150)

security_policy.output_protect {#output-protect}

Name	Value	Required	Description
allow_external_display	boolean	No	모바일 외부 출력 허용 여부. (기본값 false) NCG DRM에만 해당
control_hdcp	number	No	HDCP 적용 여부. (기본값 0) 0 : HDCP 제어 안함, 1 : HDCP 1.4 필요, 2 : HDCP 2.2 필요

external_key (optional) {#external-key}

Name	Value	Required	Description
mpeg_cenc	json	No	CENC 외부 키 정보 설정 - PlayReady/Widevine (상세 규격 참조)
hls_aes	json	No	HLS AES 외부 키 정보 설정 - FairPlay Streaming (상세 규격 참조)
ncg	json	No	NCG DRM 외부 키 정보 설정 (상세 규격 참조)

external_key.mpeg_cenc {#external-key-cenc}

Name	Value	Required	Description
key_id	hex-string	No	DASH CENC 패키징(PlayReady/Widevine) 시 사용한 key ID 16byte hex string 값
key	hex-string	No	DASH CENC 패키징 시 사용한 key 16byte hex string 값
iv	hex-string	No	DASH CENC 패키징 시 사용한 iv 16byte hex string 값

external_key.hls_aes {#external-key-aes}

Name	Value	Required	Description
key	hex-string	No	HLS Sample AES 패키징(FairPlay Streaming) 시 사용한 key 16byte hex string 값

Name	Value	Required	Description
iv	hex-string	No	HLS Sample AES 패키징 시 사용한 iv 16byte hex string 값

external_key.ncg {#external-key-ncg}

Name	Value	Required	Description
cek	hex-string	No	NCG 패키징 시 사용한 cek 32byte hex string 값

JSON 방식 예제 {#example-json}

요청 데이터

```
{
    "user_id": "test-user",
    "cid":"DEMOtest-cid",
    "oid": "",
    "nonce": "3426u3050329384g",
    "device_id": "34905esdk-39ru303h-32jd90332",
    "device_type": "android",
    "drm_type": "NCG"
}
```

응답 데이터

```
{
    "error_code": "0000",
    "error_message": "success",
    "playback_policy": {
        "limit": true,
        "persistent": true,
        "duration" : 3600
    },
    "security_policy": {
        "hardware_drm": false,
        "output_protect": {
            "allow_external_display" : true,
            "control_hdcp": 1
```

```
        },
        "allow_mobile_abnormal_device" : false,
        "playready_security_level" : 2000
    },
    "external_key": {
        "mpeg_cenc": {
            "key_id" : "00112233445566778899001122334455 66",
            "key" : "00112233445566778899001122334455 66",
            "iv" : "00112233445566778899001122334455 66"
        },
        "hls_aes" : {
            "key" : "00112233445566778899001122334455 66",
            "iv" : "00112233445566778899001122334455 66"
        },
        "ncg":{
            "cek":"30313233343536373839616263646566"
        }
    },
    "nonce": "3426u3050329384g"
}
```

라이선스 콜백 API (XML방식 구 규격) {#callback-xml}

요청 데이터 규격

- Request URI : PallyCon 콘솔 사이트의 '콘텐츠 사용 정보 URL' 세팅에 등록된 URL로 요청 됩니다.
- Request Method : POST
- Character set : UTF-8
- POST body : request parameters

Key	Value
data	base64 Encoding (aes256 Encrypt (**XML Data string**))

> [AES256 암호화 항목](#) 참조

XML 데이터 형식

```
<?xml version='1.0' encoding='utf-8'?>
<RES>
```

```
    <USERID>User ID</USERID>
    <CID>Content ID</CID>
    <OID>Optional ID</OID>
    <NONCE>Random String</NONCE>
</RES>
```

Element Name	Value	Description
USERID	string	서비스 사이트 사용자 ID
CID	string	재생하려는 콘텐츠의 ID
OID	string	부가 연동 정보. 주문 정보 등 추가적으로 서비스 사이트에 전달되기를 원하는 정보를 입력합니다. 사용 여부는 선택 사항입니다.
NONCE	enum	One time Random String. 응답을 보낼 때 동일 값으로 회신해야 합니다.

응답 데이터 규격

- body : base64 Encoding (aes256 Encrypt (**XML Data string**))

XML 데이터 형식

```
<?xml version='1.0' encoding='utf-8'?>
<RES>
    <ERROR>Error code</ERROR>
    <ERRMSG>Error Message</ERRMSG>
    <LIMIT>Y/N</LIMIT>
    <PD_START>yyyy-mm-ddThh:mm:ssZ</PD_START>
    <PD_END>yyyy-mm-ddThh:mm:ssZ</PD_END>
    <PC HDCP="0" CGMS-A="-1" APS="0"></PC>
    <PACKINFO KEYID="base64 Encoding String" KEY="base64 Encoding String" I
    <NONCE>Random String</NONCE>
</RES>
```

Element Name	Attribute	Value	Description
ERROR		string	"0000" : 성공, 에러인 경우 서비스 업체에서 정의된 에러 코드

Element Name	Attribute	Value	Description
ERRMSG		string	에러인 경우 에러 메시지
LIMIT		Y / N	무제한 권한 'N', 사용 제한 'Y'
PD_START		time	재생 가능 시작 시간, GMT Time 표기'yyyy-mm-ddThh:mm:ssZ'
PD_END		time	만료 시간, GMT Time 표기'yyyy-mm-ddThh:mm:ssZ'
PC	HDCP	number	'0' : HDCP 보안 미설정. 모든 기기 허용(기본값) '1' : HDCP 보안 설정. HDCP 지원 환경만 허용
	CGMS-A	number	Copy Generation Management System - Analog 0: Copy Freely, 1: Copy No More2: Copy Once, 3: Copy Never-1: CGMS-A Off (default)
	APS	number	Macrovision Analog Protection System 0: APS Off (default)1: AGC Only2: AGC & 2 line color stripe, 3: AGC & 4 line color stripe
PACKINFO	KEYID	string	Content Key ID, 16 byte binarybase64 encoding 문자열로 변환
	KEY	string	Content Encryption AES Key, Random 16 bytebase64 encoding 문자열로 변환
	IV	string	Content Encryption AES IV, Random 16 byte (optional)base64 encoding 문자열로 변환. IV 값은 필요한 경우만 사용.
NONCE		string	One time Random String. 요청에 포함된 것과 동일한 값으로 회신합니다.

XML 방식 예제 {#example-xml}

요청 데이터

```
<?xml version='1.0' encoding='utf-8'?>
<RES>
    <USERID>test user</USERID>
    <CID>test_content_id</CID>
    <OID>ordernumber_0001</OID>
    <NONCE>2nW8WZ0DRL8PRKRh</NONCE>
</RES>
```

응답 데이터

```
<?xml version='1.0' encoding='utf-8'?>
<RES>
    <ERROR>0000</ERROR>
    <ERRMSG>Success</ERRMSG>
    <LIMIT>Y</LIMIT>
    <PD_START>2018-08-01T10:00:00Z</PD_START>
    <PD_END>2018-08-31T24:00:00Z</PD_END>
    <PC HDCP="1" CGMS-A="-1" APS="0"></PC>
    <PACKINFO KEYID="cFvUDPTIxsRqHqRLKV1qow==" KEY="udE3LaUpven0HdcbUjs0oQ=
    <NONCE>2nW8WZ0DRL8PRKRh</NONCE>
</RES>
```

AES256 암호화 {#aes256}

AES256 암호화/복호화 처리는 PallyCon Cloud 서비스 사이트 생성 시 발급되는 사이트 키 값을 이용하여 아래와 같이 처리합니다. (PallyCon 콘솔 사이트의 셋팅 페이지에서 확인)

```
- mode : CBC
- key : 32 byte (PallyCon 서비스 사이트에서 발급되는 사이트 키)
- iv : 16 byte ( 0123456789abcdef )
- padding : pkcs7
```