PallyCon License Callback Guide v1.0

Overview {#intro}

There are two types of methods for issuing multi-DRM (FPS, Widevine, PlayReady, NCG) licenses from PallyCon cloud server.

1. Callback type

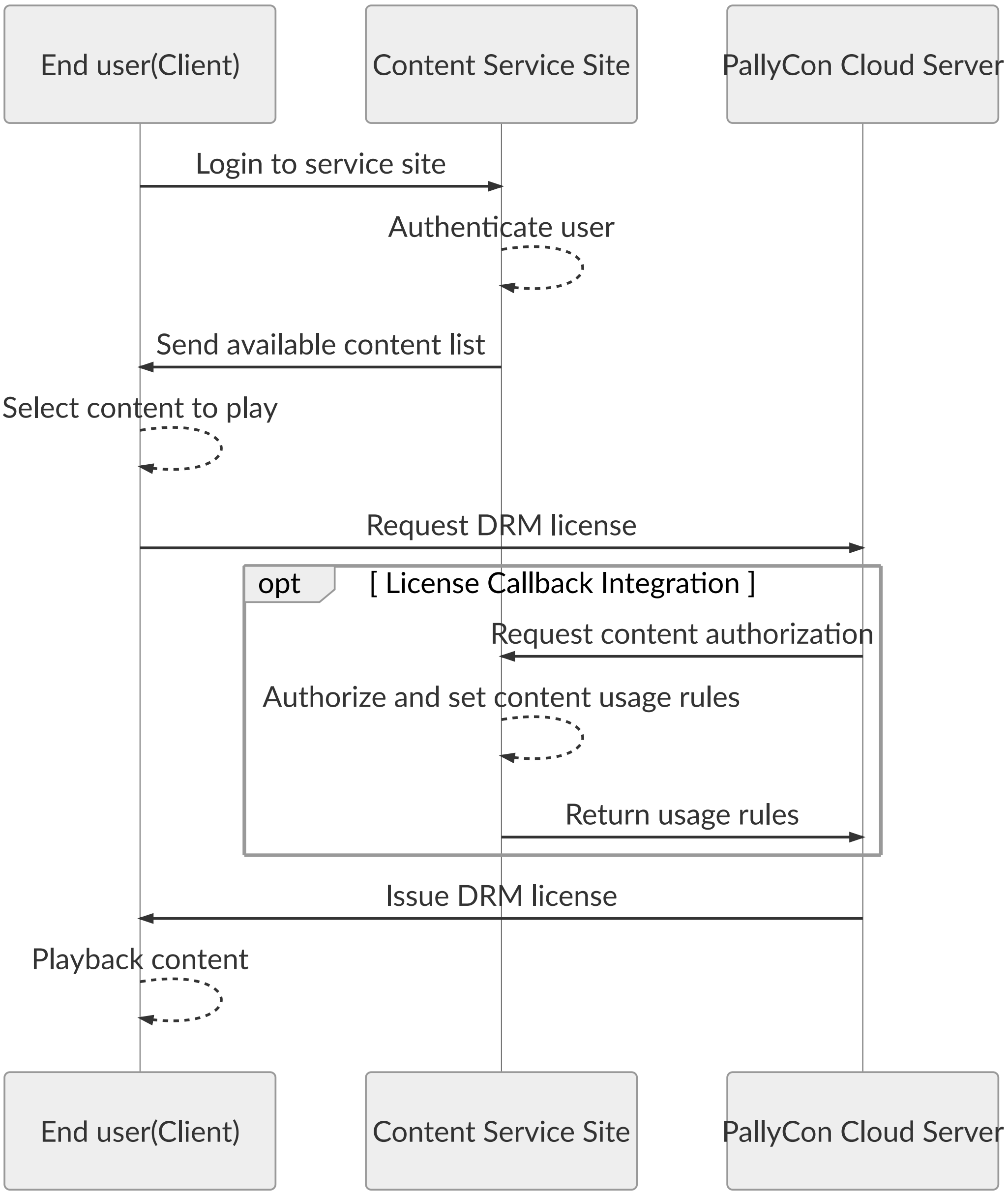
    - When PallyCon cloud server receives license request from multi-DRM client, it first checks service site's callback page to see if the user has valid permissions.
    - In the case of a request from an authorized user, the service site returns information such as authentication, usage rights (unlimited, fixed period) and various security options to the PallyCon cloud server through the callback web page.
    - PallyCon cloud server receives the response from the callback page and issues the license to the client.

2. Token type

    - When a multi-DRM client tries to play DRM content, the service site can create license token with pre-defined specification.
    - The service site can set usage rights (expiration date or unlimited) and various security options through the token data.
    - When a client requests a license with a token, the PallyCon cloud server validates the token and issues a license.

This document describes the first method, the API of license callback. Please refer to License Token Guide if you need token type integration.

License Issuance Flow {#workflow}



1. Initiate Content Playback

   - Client (Player) receives DRM integration data (PallyCon CustomData) from the service site to play DRM contents and attempts to play DRM contents.

2. Request License

   - Client requests DRM license to PallyCon cloud server.

3. Authentication via Callback (refer to callback spec)

   - PallyCon cloud server makes a user authentication request to the corresponding service site.

4. Respond usage rights info

    - The service site responds content usage rights info after authenticating the user on the callback page.

5. Issue license

    - PallyCon Cloud server generates and issues the license information received from the callback page in a license that matches the DRM type (FPS, Widevine, PlayReady and NCG).

License Callback API (JSON type) {#callback-json}

Request Data Spec

- Request URI : requested at the URL which is registered in the ‘Content usage information URL’ setting on the PallyCon Console site.

- Request Method : POST

- Character set : UTF-8

- POST body : request parameters

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

* **refer to AES256 encryption section**

JSON Data Format

```
{
    "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	Service site's user ID
cid	string	Yes	Unique ID of content. Max 200 bytes alphanumeric string
oid	string	No	Optional data (such as order info) which needs to be sent to service site for the integration.
nonce	string	Yes	One time Random String. It should be the same as in response data
device_id	string	No	Client device's ID (for NCG DRM only)
device_type	string	No	Type of client device(for NCG DRM only) OS-X, Windows, Android, iOS
drm_type	string	Yes	Type of DRM ("NCG", "Widevine", "PlayReady", "FairPlay")

Response Data Format

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

JSON Data Format

```
{
    "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" : Success. In case of failure, numeric error code defined by service site.
error_message	string	Yes	Contains error message in case of failure.
response_user_id	string	No	Changes the user ID included in the license request to a separate ID that is answered by the callback. Use when the client does not know the user ID information of the service. (optional)
playback_policy	json	Yes	license rules related with playback (refer to spec)
security_policy	json	No	license rules related with security (refer to spec)
external_key	json	No	Uses external content key to generate license. (refer to spec)
nonce	string	Yes	One time Random String. Should be the same string as in the request data.

playback_policy {#playback-policy}

Name	Value	Required	Description
limit	boolean	No	whether playback period is limited (default: false) true : limited playback period, false : unlimited
persistent	boolean	No	whether the license is persistent. (default: false) true : keep license, false : remove license after play(for streaming)
duration	number	Select	duration of playback (unit: second). **'expire_date' is ignored if 'duration' is set.** 'limit' should be true to apply this setting.
expire_date	string	Select	date of license expiration, GMT Time 'yyyy-mm-ddThh:mm:ssZ' 'limit' should be true to apply this setting. This setting cannot be used with 'duration'.

security_policy (optional) {#security-policy}

Name	Value	Required	Description
hardware_drm	boolean	No	Whether hardware DRM is required.(default: false) valid for CENC (Widevine Modular) contents only
output_protect	json	No	settings for external display (refer to spec)
allow_mobile_abnormal_device	boolean	No	whether rooted device is allowed (default: false)
playready_security_level	number	No	Security level of PlayReady DRM, 150,2000 (default: 150)

security_policy.output_protect {#output-protect}

Name	Value	Required	Description
allow_external_display	boolean	No	Whether external display is allowed. (default: false) valid for NCG DRM only
control_hdcp	number	No	Setting for applying HDCP. (default: 0) 0 : No HDCP, 1 : HDCP 1.4, 2 : HDCP 2.2

external_key (optional) {#external-key}

Name	Value	Required	Description
mpeg_cenc	json	No	CENC external key setting for PlayReady/Widevine (refer to spec)
hls_aes	json	No	HLS AES external key setting for FairPlay Streaming (refer to spec)
ncg	json	No	NCG DRM external key setting (refer to spec)

external_key.mpeg_cenc {#external-key-cenc}

Name	Value	Required	Description
key_id	hex-string	No	Key ID for DASH CENC packaging(PlayReady/Widevine) 16byte hex string
key	hex-string	No	Key for DASH CENC packaging 16byte hex string
iv	hex-string	No	IV for DASH CENC packaging. 16byte hex string

external_key.hls_aes {#external-key-aes}

Name	Value	Required	Description
key	hex-string	No	Key for HLS Sample AES packaging(FairPlay Streaming) 16byte hex string
iv	hex-string	No	IV for HLS Sample AES packaging. 16byte hex string

external_key.ncg {#external-key-ncg}

Name	Value	Required	Description
cek	hex-string	No	CEK for NCG packaging. 32byte hex string

JSON Example {#example-json}

Request Data

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

Response Data

```
{
    "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" : "0011223344556677889900112233445566",
            "key" : "0011223344556677889900112233445566",
            "iv" : "0011223344556677889900112233445566"
        },
        "hls_aes" : {
            "key" : "0011223344556677889900112233445566",
            "iv" : "0011223344556677889900112233445566"
        },
        "ncg":{
            "cek":"30313233343536373839616263646566"
        }
    },
    "nonce": "3426u3050329384g"
}
```

License Callback API (XML type old spec) {#callback-xml}

Request Data Format

- Request URI : requested at the URL registered in the ‘Content usage info URL’ setting on the PallyCon Console site.
- Request Method : POST
- Character set : UTF-8
- POST body : request parameters

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

* **Refer to AES256 encryption**

XML Data Format

```xml
<?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	ID of content service site user
CID	string	Unique ID of the content
OID	string	Optional data (such as order info) which needs to be sent to service site for the integration.
NONCE	enum	One time Random String. It should be the same string as in the response data.

Response Data Format

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

XML Data Format

```xml
<?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	Success: 0000, Failure: 4byte error code other than 0000 (defined by content service site)
ERRMSG		string	Description of the error
LIMIT		Y / N	Unlimited playback 'N', Limited playback period 'Y'
PD_START		time	Start of playback period, GMT Time 'yyyy-mm-ddThh:mm:ssZ'
PD_END		time	End of playback period, GMT Time 'yyyy-mm-ddThh:mm:ssZ'
PC	HDCP	number	Flag to enable HDCP for digital output protection. 0: Allow non-HDCP playback (default), 1: HDCP playback only
	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 binary -> base64 encoding
	KEY	string	Content Encryption AES Key, Random 16 byte string -> base64 encoding
	IV	string	Content Encryption AES IV, Random 16 byte string -> base64 encoding (optional)
NONCE		string	One time Random String. It should be the same string as in the request data.

XML Example {#example-xml}

Request Data

```
<?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>
```

Response Data

```
<?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 Encryption {#aes256}

```
AES256 Encryption
- mode : CBC
- key : 32 byte (Site key from PallyCon Console site)
- iv : 16 byte (0123456789abcdef)
- padding : pkcs7
```

AES256 Encryption/Decryption should be processed as below using site authentication key which is created by ‘Service Request’ on PallyCon Console site. (The key can be found on PallyCon Console’s settings page)