

Recommendation

ITU-T J.1042 (03/2025)

SERIES J: Cable networks and transmission of television, sound programme and other multimedia signals

Conditional access and protection – Digital rights management for video and audio content distribution

Digital rights management for video and audio content distribution – Client

ITU-T J-SERIES RECOMMENDATIONS
Cable networks and transmission of television, sound programme and other multimedia signals

GENERAL RECOMMENDATIONS	J.1-J.9
GENERAL SPECIFICATIONS FOR ANALOGUE SOUND-PROGRAMME TRANSMISSION	J.10-J.19
PERFORMANCE CHARACTERISTICS OF ANALOGUE SOUND-PROGRAMME CIRCUITS	J.20-J.29
EQUIPMENT AND LINES USED FOR ANALOGUE SOUND-PROGRAMME CIRCUITS	J.30-J.39
DIGITAL ENCODERS FOR ANALOGUE SOUND-PROGRAMME SIGNALS - PART 1	J.40-J.49
DIGITAL TRANSMISSION OF SOUND-PROGRAMME SIGNALS	J.50-J.59
CIRCUITS FOR ANALOGUE TELEVISION TRANSMISSION	J.60-J.69
ANALOGUE TELEVISION TRANSMISSION OVER METALLIC LINES AND INTERCONNECTION WITH RADIO-RELAY LINKS	J.70-J.79
DIGITAL TRANSMISSION OF TELEVISION SIGNALS	J.80-J.89
ANCILLARY DIGITAL SERVICES FOR TELEVISION TRANSMISSION	J.90-J.99
OPERATIONAL REQUIREMENTS AND METHODS FOR TELEVISION TRANSMISSION	J.100-J.109
INTERACTIVE SYSTEMS FOR DIGITAL TELEVISION DISTRIBUTION (DOCSIS FIRST AND SECOND GENERATIONS)	J.110-J.129
TRANSPORT OF MPEG-2 SIGNALS ON PACKETIZED NETWORKS	J.130-J.139
MEASUREMENT OF THE QUALITY OF SERVICE - PART 1	J.140-J.149
DIGITAL TELEVISION DISTRIBUTION THROUGH LOCAL SUBSCRIBER NETWORKS	J.150-J.159
IPCABLECOM (MGCP-BASED) - PART 1	J.160-J.179
DIGITAL TRANSMISSION OF TELEVISION SIGNALS - PART 1	J.180-J.189
CABLE MODEMS AND HOME NETWORKING	J.190-J.199
APPLICATION FOR INTERACTIVE DIGITAL TELEVISION - PART 1	J.200-J.209
INTERACTIVE SYSTEMS FOR DIGITAL TELEVISION DISTRIBUTION (DOCSIS THIRD TO FIFTH GENERATIONS)	J.210-J.229
MULTI-DEVICE SYSTEMS FOR CABLE TELEVISION	J.230-J.239
MEASUREMENT OF THE QUALITY OF SERVICE - PART 2	J.240-J.249
DIGITAL TELEVISION DISTRIBUTION THROUGH LOCAL SUBSCRIBER NETWORKS	J.250-J.259
IPCABLECOM (MGCP-BASED) - PART 2	J.260-J.279
DIGITAL TRANSMISSION OF TELEVISION SIGNALS - PART 2	J.280-J.289
CABLE SET-TOP BOX	J.290-J.299
APPLICATION FOR INTERACTIVE DIGITAL TELEVISION - PART 2	J.300-J.309
MEASUREMENT OF THE QUALITY OF SERVICE - PART 3	J.340-J.349
IPCABLECOM2 (SIP-BASED) - PART 1	J.360-J.379
DIGITAL TRANSMISSION OF TELEVISION SIGNALS - PART 3	J.380-J.389
MEASUREMENT OF THE QUALITY OF SERVICE - PART 4	J.440-J.449
IPCABLECOM2 (SIP-BASED) - PART 2	J.460-J.479
DIGITAL TRANSMISSION OF TELEVISION SIGNALS - PART 4	J.480-J.489
TRANSPORT OF LARGE SCREEN DIGITAL IMAGERY	J.600-J.699
SECONDARY DISTRIBUTION OF IPTV SERVICES	J.700-J.799
MULTIMEDIA OVER IP IN CABLE	J.800-J.899
TRANSMISSION OF 3-D TV SERVICES	J.900-J.999
CONDITIONAL ACCESS AND PROTECTION	J.1000-J.1099
Renewable conditional access system	J.1000-J.1004
Digital rights management for cable television multiscreen service	J.1005-J.1009
Exchangeable embedded conditional access and digital rights management solutions	J.1010-J.1019
Downloadable system for multi-CA/DRM service of mobile broadcasting	J.1020-J.1025
Downloadable conditional access system for unidirectional networks	J.1026-J.1029
Downloadable conditional access system for bidirectional networks	J.1031-J.1035
Factual subscriber-base reporting and protected content delivery in conditional access systems	J.1036-J.1039
Digital rights management for video and audio content distribution	J.1040-J.1044
SWITCHED DIGITAL VIDEO OVER CABLE NETWORKS	J.1100-J.1119
SMART TV OPERATING SYSTEM	J.1200-J.1209
IP VIDEO BROADCAST	J.1210-J.1219
CABLE SET-TOP BOX - PART 2	J.1290-J.1299
CLOUD-BASED CONVERGED MEDIA SERVICES FOR IP AND BROADCAST CABLE TELEVISION	J.1300-J.1309
CLOUD-BASED SERVICES FOR IP DELIVERY OVER INTEGRATED BROADBAND CABLE NETWORK	J.1310-J.1319
TELEVISION TRANSPORT NETWORK AND SYSTEM DEPLOYMENT IN DEVELOPING COUNTRIES	J.1400-J.1409
ARTIFICIAL INTELLIGENCE (AI) ASSISTED CABLE NETWORKS	J.1600-J.1649

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T J.1042

Digital rights management for video and audio content distribution – Client

Summary

Recommendation ITU-T J.1042 is Part 3 of a multi-part deliverable composed of four parts. Part 3 describes the client framework and defines related interfaces of digital rights management for video and audio content distribution (DRMVACD). These interfaces include digital rights management (DRM) function interfaces and client execution environment interfaces.

The service requirements for the application of new generation video and audio technologies, along with new video service models coupled with a diverse range of consumer devices used for the reception of content, bring new demands and opportunities to the video industry, especially broadcast and television video services, and raise higher requirements for DRM, described in Recommendation ITU-T J.1040. The DRM system not only needs to have well defined security levels to meet the content protection requirements of different quality and different distribution window periods but also needs to have sufficient platform compatibility to cover various terminal devices. In addition, higher encryption/decryption efficiency and encryption/decryption modes decoupled from content encapsulation are required to match the rapid development and transformation of video and audio technologies. In addition, an interoperability mechanism is required to achieve a more open DRM ecosystem.

History^{*}

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T J.1042	2025-03-16	21	11.1002/1000/16263

Keywords

Digital rights management, DRM Client, video and audio content distribution, video and audio content protection.

^{*} To access the Recommendation, type the URL <https://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, and information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at <https://www.itu.int/ITU-T/ipr/>.

© ITU 2025

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

	Page
1 Scope	1
2 References.....	1
3 Definitions	1
3.1 Terms defined elsewhere	1
3.2 Terms defined in this Recommendation.....	1
4 Abbreviations and acronyms	1
5 Conventions	2
6 DRM client	2
6.1 DRM application module	4
6.2 DRM function module.....	4
6.3 DRM client execution environment	4
6.4 DRM function interface.....	4
6.5 DRM client execution environment interface	4
Annex A – DRM client function interface.....	5
A.1 Constant definitions.....	5
A.2 Data structure definitions	6
A.3 Interface definitions.....	7
A.4 Interface invoking process.....	11
Annex B – DRM client execution environment interface.....	12
B.1 Constant definitions.....	12
B.2 Data structure definitions	14
B.3 Interface definitions.....	18
Bibliography.....	36

Introduction

This Recommendation document is Part 3 of a multi-part deliverable composed of four parts. Part 3 describes the client framework and defines related interfaces of digital rights management (DRM) for video and audio content distribution (DRMVACD). These interfaces include DRM function interfaces and client execution environment interfaces. The other parts are identified below:

Part 1: Requirements;

Part 2: System Architecture;

Part 3: Client;

Part 4: Compliance and Robustness Rules.

Recommendation ITU-T J.1042

Digital rights management for video and audio content distribution – Client

1 Scope

This Recommendation is part 3 of a multiparty deliverable composed of four parts. Part 3 describes the client framework and defines related interfaces of digital rights management (DRM) for video and audio content distribution. The DRM requirements are described in [ITU-T J.1040].

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[[ITU-T J.1040](#)] Recommendation ITU-T J.1040 (2024), *Digital rights management for video and audio content distribution - Requirements*.

[[ITU-T J.1041](#)] Recommendation ITU-T J.1041 (2025), *Digital rights management for video and audio content distribution – System Architecture*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 digital rights management (DRM) client [ITU-T J.1040]: A trusted entity in the digital media content playback device responsible for execution of DRM content-related permissions and restrictions.

3.1.2 digital rights management (DRM) content [ITU-T J.1040]: Digital media content managed by DRM technology.

3.1.3 encryption [b-ITU-T X.1367]: The cryptographic transformation of data to produce ciphertext.

3.1.4 decryption [b-ITU-T Y.101]: The decoding of encrypted information.

3.1.5 license [ITU-T J.1040]: A description of control information such as access permissions, usage rules, and keys for digital media content.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CBC Cipher Block Chain

CENC Common Encryption

DRM	Digital Rights Management
DRMVACD	DRM for Video and Audio Content Distribution
HMAC	Hash-based Message Authentication Code

5 Conventions

In this Recommendation:

The keywords "**is required to**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this Recommendation is to be claimed.

The keywords "**is recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

The keywords "**is prohibited from**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this Recommendation is to be claimed.

The keywords "**can optionally**" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

In this Recommendation, the words shall, shall not, should and may sometimes appear, in which case they are to be interpreted, respectively, as is required to, is prohibited from, is recommended, and can optionally. The appearance of such phrases or keywords in an appendix or in material explicitly marked as informative are to be interpreted as having no normative intent.

6 DRM client

The digital rights management (DRM) client is a trusted entity on a device that enforces the permissions and restrictions associated with DRM content. It is an essential part of DRM for video and audio content distribution (DRMVACD), whose functional architecture can be seen in Figure 1 in [ITU-T J.1041]. The DRM client includes the DRM application module, the DRM function module, the DRM client execution environment, the DRM function interface, and the DRM client execution environment interface. The DRM client framework is shown in Figure 1.

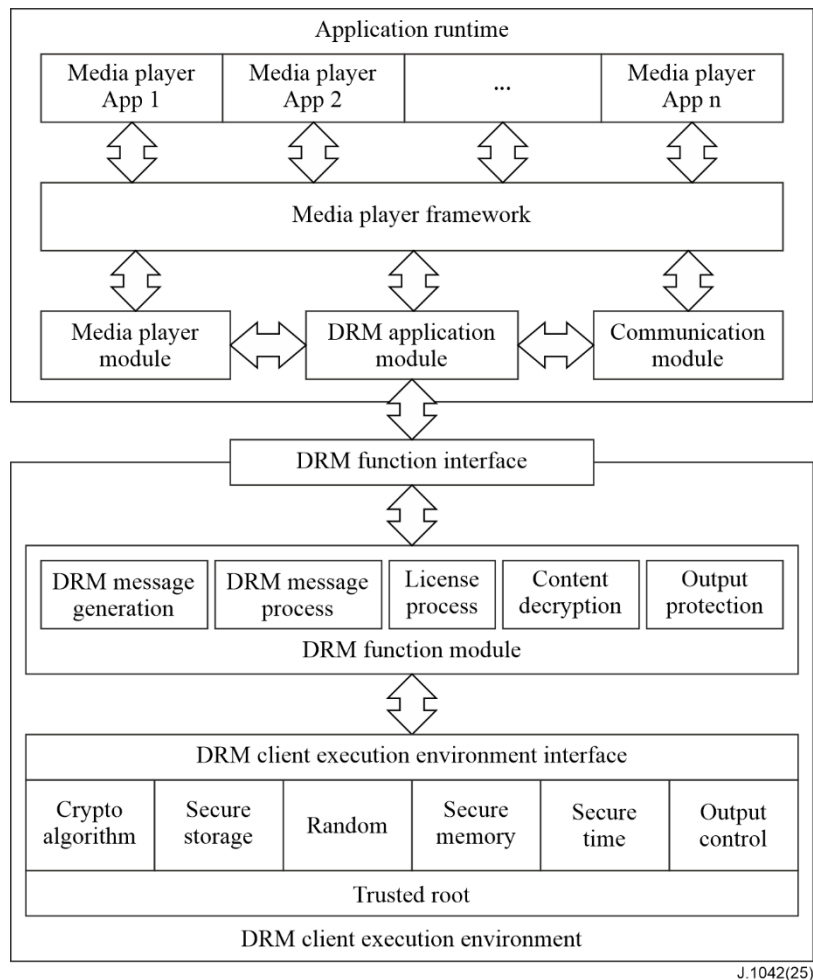


Figure 1 – DRM client framework

The DRM application module shall be responsible for integrating the DRM function with applications such as the media player. The DRM client application module integrates with the media player framework to enable the media player application to support the DRM function. The DRM function is implemented by invoking the DRM function interface.

The DRM function module shall provide DRM function for the DRM application module. The DRM function module runs in the DRM client execution environment. It implements the core functions of the DRM client by invoking the DRM client execution environment interface.

The DRM client execution environment shall provide security capability for the DRM function module, providing the basic security assurance for establishing DRM client trust and a security system, and executing DRM client core functions, etc.

The DRM client is classified into three security levels: software security level, hardware security level, and enhanced hardware security level. Software security level requires that part or all of the DRM client execution environment be implemented based on the software security mechanism; hardware security level requires that the DRM client execution environment be implemented based on the hardware security mechanism; based on the hardware security level, enhanced hardware security level also requires that the DRM client execution environment possess capabilities including side-channel attack resistance and forensic watermark.

6.1 DRM application module

The DRM application module runs in the application execution environment and is a logical module for media related applications to integrate DRM client functions. The DRM application module invokes the DRM function module through the DRM function interface to protect the content.

6.2 DRM function module

The DRM function module shall be executed in the DRM client execution environment, and supports DRM message generation, DRM message processing, license processing, content decryption, output protection, and DRM client private key and certificates provisioning function.

The DRM client private key, content encryption key and content authorization license shall be stored securely in the DRM client execution environment, and can be used only in the DRM client execution environment.

6.3 DRM client execution environment

The DRM client execution environment shall support root of trust, cryptographic algorithms, secure storage, random number generation, secure memory, secure time and output control. If the DRM client private key and certificates are not provisioned into the chipset or device before delivery, the DRM client execution environment must have a secure provisioning function for the DRM client private key and certificates.

The DRM client execution environment shall be able to protect its own integrity and the integrity of the DRM function module. Before the DRM function module runs, the DRM client execution environment shall be able to verify the integrity of the DRM function module to prevent the DRM core functionality from being tampered with.

The DRM function module runs in the DRM client execution environment. This execution environment is a logical module which can be implemented based on the chipset hardware security execution environment (such as TEE), based on the software security execution environment (such as WhiteBox), or implemented based on a combined secure execution environment consisting of both software and hardware.

6.4 DRM function interface

The DRM function interface is an interface provided by the DRM function module in the DRM client execution environment for integration with the DRM application module. The definition of the interface is shown in Annex A.

6.5 DRM client execution environment interface

The DRM client execution environment interface is the DRM security capability interface provided by the DRM client execution environment for the DRM function module, including cryptographic algorithms, secure storage, random number, secure memory, secure time, output control, etc. The definition of DRM client execution environment interface is shown in Annex B.

Annex A

DRM client function interface

(This annex forms an integral part of this Recommendation.)

A.1 Constant definitions

A.1.1 Authorization status CDRMC_Rights_Status

Prototype:

```
typedef enum {  
    CDRMC_RIGHTS_VALID = 0x00,  
    CDRMC_RIGHTS_INVALID = 0x01,  
    CDRMC_RIGHTS_NOT_ACQUIRED = 0x02,  
    CDRMC_RIGHTS_EXPIRED = 0x03,  
} CDRMC_Rights_Status;
```

Description:

Authorization status.

Members:

- CDRMC_RIGHTS_VALID: valid permission;
- CDRMC_RIGHTS_INVALID: invalid permission;
- CDRMC_RIGHTS_NOT_ACQUIRED: no permission;
- CDRMC_RIGHTS_EXPIRED: permission expired.

A.1.2 Algorithms and modes of symmetric encryption and decryption CDRMC_Symmetric_Crypto_Algorithm

Prototype:

```
typedef enum {  
    CDRMC_ALG_SM4_CBC_NOPAD = 0x01,  
    CDRMC_ALG_SM4_CTR = 0x02,  
} CDRMC_Symmetric_Crypto_Algorithm;
```

Description:

The algorithms and modes of symmetric encryption and decryption.

Members:

- CDRMC_ALG_SM4_CBC_NOPAD: SM4_CBC mode;
- CDRMC_ALG_SM4_CTR: SM4_CTR mode.

A.1.3 Common encryption (CENC) algorithms and modes CDRMC_Cenc_Algorithm

Prototype:

```
typedef enum {  
    CDRMC_ALG_CENC_SM4_CTR = 0x03,  
    CDRMC_ALG_CENC_SM4_CBC = 0x04,  
} CDRMC_Cenc_Algorithm;
```

Description:

CENC algorithms and modes.

Members:

- CDRMC_ALG_CENC_SM4_CTR: SM4-CTR mode;
- CDRMC_ALG_CENC_SM4_CBC: SM4-CBC mode.

A.2 Data structure definitions

A.2.1 DRM session handle structure CDRMC_SessionHandle

Prototype:

```
typedef void* CDRMC_SessionHandle;
```

Description:

DRM Session handle structure.

Member:

None.

A.2.2 CENC subsample structure CDRMC_SubSample

Prototype:

```
typedef struct __CDRMC_SubSample
{
    unsigned int u32ClearHeaderLen,
    unsigned int u32PayLoadLen,
} CDRMC_SubSample;
```

Description:

CENC subsample structure.

Members:

- u32ClearHeaderLen: the length of clear data in this subsample;
- u32PayLoadLen: the length of encrypted data in this subsample.

A.2.3 CENC data structure CDRMC_Cenc

Prototype:

```
typedef struct __CDRMC_Cenc
{
    unsigned int u32KeyIdLen,
    unsigned char * pu8KeyId,
    unsigned int u32IVLen,
    unsigned char * pu8IV,
    unsigned int u32FirstEncryptOffset,
    CDRMC_SubSample * pstSubSample,
    unsigned int u32SubsampleNum,
} CDRMC_Cenc;
```

Description:

CENC structure.

Members:

- u32KeyIdLen: the length of key identifier;
- pu8KeyId: key identifier;
- u32IVLen: the length of initialization vector;
- pu8IV: Initialization vector;
- u32FirstEncryptOffset: the length of initial offset of encrypted data;
- pstSubSample: subsample description;
- u32SubsampleNum: the number of subsamples.

A.3 Interface definitions

A.3.1 CDRMC_OpenSession

Prototype:

```
int CDRMC_OpenSession (CDRMC_SessionHandle *phSession);
```

Function:

Create a DRM session.

Parameter:

- phSession -output parameter, DRM session handle.

Return:

int, 0 indicates success and other values indicate failure.

A.3.2 CDRMC_CloseSession

Prototype:

```
int CDRMC_CloseSession (CDRMC_SessionHandle hSession).
```

Function:

Close a DRM session.

Parameter:

- hSession -input parameter, DRM session handle.

Return:

int, 0 indicates success and other values indicate failure.

A.3.3 CDRMC_GetLicenseRequest

Prototype:

```
int CDRMC_GetLicenseRequest (CDRMC_SessionHandle hSession, unsigned char*  
pu8DrmInfo, unsigned int u32DrmInfoLen, unsigned char* pu8LicenseRequest, unsigned  
int* pu32LicenseRequestLen);
```

Function:

Get the license request message.

Parameters:

- hSession -input parameter, DRM session handle;
- pu8DrmInfo -input parameter, DRM information of encrypted content;
- u32DrmInfoLen -input parameter, the length of DRM information of encrypted content;
- pu8LicenseRequest -output parameter, license request data buffer;

- pu32LicenseRequestLen -input and output parameter, the length of the license request data buffer as input, and the length of the license request data as output.

Return:

int, 0 indicates success and other values indicate failure.

A.3.4 CDRMC_ProcessLicenseResponse

Prototype:

```
int CDRMC_ProcessLicenseResponse (CDRMC_SessionHandle hSession, unsigned char*
pu8LicenseResponse, unsigned int u32LicenseResponseLen);
```

Function:

Process license response message.

Parameters:

- hSession -input parameter, DRM session handle;
- pu8LicenseResponse -input parameter, license data;
- u32LicenseResponseLen -input parameter, the length of license data.

Return:

int, 0 indicates success and other values indicate failure.

A.3.5 CDRMC_GetProvisionRequest

Prototype:

```
int CDRMC_GetProvisionRequest (CDRMC_SessionHandle hSession, unsigned char*
pu8ProvisionRequest, unsigned int* pu32ProvisionRequestLen);
```

Function:

Get the certificate request message.

Parameters:

- hSession -input parameter, DRM session handle;
- pu8ProvisionRequest -output parameter, the certificate request data buffer;
- pu32ProvisionRequestLen -input and output parameter, the length of the certificate request data buffer as input, and the length of the certificate request data as output.

Return:

int, 0 indicates success and other values indicate failure.

A.3.6 CDRMC_ProcessProvisionResponse

Prototype:

```
int CDRMC_ProcessProvisionResponse (CDRMC_SessionHandle hSession, unsigned
char* pu8ProvisionResponse, unsigned int u32ProvisionResponseLen);
```

Function:

Process the certificate response message.

Parameters:

- hSession -input parameter, DRM session handle;
- pu8ProvisionResponse -input parameter, certificate data;
- u32ProvisionResponseLen -input parameter, the length of certificate data.