CLAIMS

1. A digital rights management (DRM) method of media content implemented in a terminal device, on which a DRM client is installed, the method comprising:

step 1: receiving by the DRM client an invoking request of a media application of the terminal device, and acquiring by the DRM client a unique identifier of media content to be played from the invoking request;

step 2: sending, by the DRM client, a DRM authorization request to a DRM server side so as to acquire a content authorization execution unit, wherein the DRM authorization request contains an identifier of the media content and basic information of the DRM client, wherein

the content authorization execution unit is generated by the DRM server side in the following way: the DRM server side obtains a content encryption algorithm and a content encryption key which are adopted by the media content, and DRM authority of the DRM client to the media content according to the DRM authorization request through query, and is then generated according to the identifier of the media content, the content encryption algorithm and the content encryption key which are adopted by the media content, the basic information of the DRM client, and the DRM authority of the DRM client to the media content; and

step 3, by the DRM client, running the content authorization execution unit in a DRM client running environment, verifying whether a terminal running environment conforms to the DRM authority of the DRM client to the media content through the content authorization execution unit, and if so, decrypting the media content according to the content encryption algorithm and the content encryption key,

wherein, the DRM client further comprises an execution unit engine and an execution unit scheduling and management module, the DRM client schedules and manages execution units through the execution unit scheduling and management module, comprising scheduling the execution unit to the execution unit engine for running, the execution units comprise the content authorization execution unit.

2. A digital rights management (DRM) method of media content implemented in a DRM server side, the method comprising:

step 1: receiving, by the DRM server side, a DRM authorization request sent by a DRM client, wherein the DRM authorization request contains a unique identifier of the media

content and basic information of the DRM client;

step 2: obtaining, by the DRM server side, a content encryption algorithm and a content encryption key which are adopted by the media content, and DRM authority of the DRM client to the media content according to the DRM authorization request through query;

step 3, generating, by the DRM server side, a content authorization execution unit according to an identifier of the media content, the content encryption algorithm and the content encryption key which are adopted by the media content, the basic information of the DRM client, and the DRM authority of the DRM client to the media content, wherein the content authorization execution unit is configured to run in a DRM client running environment so as to verify whether a terminal running environment of a terminal device where the DRM client is located conforms to the DRM authority of the DRM client to the media content, and if so, decrypt the media content according to the content encryption algorithm and the content encryption key; and

step 4: issuing, by the DRM server side, the generated content authorization execution unit to the DRM client,

wherein, the DRM client further comprises an execution unit engine and an execution unit scheduling and management module, the DRM client schedules and manages execution units through the execution unit scheduling and management module, comprising scheduling the execution unit to the execution unit engine for running, the execution units comprise the content authorization execution unit.

3. A DRM client arranged in a terminal device, in which an intelligent operating system is installed, the DRM client comprising a media application interface, an execution unit acquisition module and a content authorization execution unit, wherein

the media application interface is configured to receive an invoking request of a media application of the terminal device and acquire a unique identifier of media content to be played from the invoking request;

the execution unit acquisition module is configured to send a DRM authorization request to a DRM server side so as to acquire the content authorization execution unit, wherein the DRM authorization request contains an identifier of the media content and basic information of the DRM client; and

the content authorization execution unit is configured to verify whether a terminal running environment conforms to DRM authority of the DRM client to the media content, and if so, decrypt the media content according to a content encryption algorithm and a

content encryption key, wherein

the content authorization execution unit is generated by the DRM server side in the following way: the DRM server side obtains the content encryption algorithm and the content encryption key which are adopted by the media content, and the DRM authority of the DRM client to the media content according to the DRM authorization request through query, and is then generated according to the identifier of the media content, the content encryption algorithm and the content encryption key which are adopted by the media content, the basic information of the DRM client, and the DRM authority of the DRM client to the media content; and

the DRM client further comprises an execution unit engine and an execution unit scheduling and management module, the DRM client schedules and manages execution units through the execution unit scheduling and management module, comprising scheduling the execution unit to the execution unit engine for running, the execution units comprise the content authorization execution unit.

4. The DRM client according to claim 3, further comprising an execution unit signature checking module configured to check the signature of the content authorization execution unit.

5. The DRM client according to claim 3 or 4, further comprising a terminal operating system adaptation module, wherein

the terminal operating system adaptation module is configured to adapt the execution unit engine to a terminal operating system.

6. The DRM client according to any of claims 3-5, wherein the execution unit engine is configured to provide a memory management interface, an external storage management interface, a network management interface, a cryptographic algorithm interface, a playing control interface and an output control interface for the running of the execution unit; and

the terminal operating system adaptation module is configured to adapt the memory management interface, the external storage management interface, the network management interface, the cryptographic algorithm interface, the playing control interface and the output control interface of the execution unit engine to corresponding interfaces of the terminal operating system.

7. The DRM client according to any of claims 3-6, wherein

the execution unit scheduling and management module is further configured to add, delete and update the execution unit; and

the execution units comprise a communication execution unit and a digital watermark execution unit.

8. A DRM server side comprising a DRM message receiving module, a media content-related DRM information acquisition module, an execution unit generation module, and an execution unit issuing module, wherein

the DRM message receiving module is configured to receive a DRM authorization request sent by a DRM client, wherein the DRM authorization request contains a unique identifier of media content and basic information of the DRM client;

the media content-related DRM information acquisition module is configured to obtain a content encryption algorithm and a content encryption key which are adopted by the media content, and DRM authority of the DRM client to the media content according to the DRM authorization request through query;

the execution unit generation module is configured to generate a content authorization execution unit according to an identifier of the media content, the content encryption algorithm and the content encryption key which are adopted by the media content, the basic information of the DRM client, and the DRM authority of the DRM client to the media content and in accordance with a content authorization execution unit template corresponding to the media content, wherein the content authorization execution unit is configured to run in a DRM client running environment so as to verify whether a terminal running environment of a terminal device where the DRM client is located conforms to the DRM authority of the DRM client to the media content and if so, decrypt the media content according to the content encryption algorithm and the content encryption key; and

the execution unit issuing module is configured to issue the content authorization execution unit to the DRM client,

wherein, the DRM client further comprises an execution unit engine and an execution unit scheduling and management module, the DRM client schedules and manages execution units through the execution unit scheduling and management module, comprising scheduling the execution unit to the execution unit engine for running, the execution units comprise the content authorization execution unit.

9. The DRM server side according to claim 8, further comprising an execution unit signature module configured to sign the content authorization execution unit before the execution unit issuing module issues the content authorization execution unit.

10. The DRM server side according to claim 8 or 9, further comprising an execution unit template management module configured to manage the content authorization execution unit template, comprising adding, updating and deleting the content authorization execution unit template.