Title: METHODS AND DEVICES FOR MANAGING CONTENT

FIG. 9

Abstract: This invention presents methods and devices for managing encrypted content. A first device generates a license data comprising a right-related data, a priority data and a content key for decrypting an encrypted content. The priority data defines the priority level of the right defined by the right-related data. A second device decrypts an encrypted content key and encrypts the content key with a second key associated with a third device. The third device receives a license data comprising a first right-related data defining a first right of using an encrypted content and a second right-related data defining a second right of using the encrypted content; and obtains a priority data defining the priority levels of the first right and the second right. In this way, it can be guaranteed that the content can be used by the third device in a way determined by both the first device and the second device.
METHODS AND DEVICES FOR MANAGING CONTENT

FIELD OF THE INVENTION

The invention relates to methods and devices for managing digital content, in particular to methods and devices for managing encrypted content in a DRM (Digital Rights Management) system.

BACKGROUND OF THE INVENTION

DRM is an access control technology that can be used by hardware manufacturers, publishers, copyright holders and individuals to try to impose limitations on the usage of digital content and devices.

In a traditional IPTV (Internet Protocol Television) video-on-demand content delivery system, several roles are involved, including a content provider, an operator and an end user. The content provider, such as a TV station, produces different types of content including entertainment and news etc. The operator, such as a telecom operator, has a physical network for distributing the content. To deliver content to an STB (Set Top Box) of an end user, the content provider has to ask for the help from the operator, because the operator has the physical network to deliver the content to end users. The general process is as follows: the content provider prepares content and delivers the content to the operator; and then the operator distributes the protected content to the STB on demand.

SUMMARY OF THE INVENTION

It has been found that the business model between a content provider and an operator may be different from the business model between an operator and an end user, and it is difficult to ensure that the operator will distribute the content exactly according to its business contract with the content provider.
For example, a content provider provides content to an operator and declares a usage limitation in the contract signed by the content provider and the operator. The usage limitation can be a capacity limitation, such as the content can be distributed only to no more than 1 million users, or a time limitation, such as the content is only available in the Chinese New Year period, while the operator has multiple options, such as pay per month and pay per view etc, for providing the content to end users. The operator should follow the business contract signed with the content provider for distributing the content, but there is no technique solution to enforce the operator to act strictly according to the contract.

It would be advantageous to be able to guarantee the content provider's rights on the content by a technique solution instead of only by a law. It would also be desirable that the technique solution can be implemented easily.

In the following, a first device corresponds to a content provider; a second device corresponds to an operator; and a third device corresponds to an end user.

To better address one or more of the above concerns, according to an embodiment of a first aspect of the present invention, a method of managing encrypted content by a first device is proposed. The method comprises the steps of:

- determining a right-related data and a priority data, said right-related data defining a right of using said encrypted content, said priority data defining the priority level of said right; and

- generating a license data comprising the right-related data, the priority data and a content key for decrypting said encrypted content, said license data being intended to authorize a second device to use said encrypted content.

By applying the license data comprising the right-related data, the priority data and the content key, the first device can authorize the second device to use the encrypted content. The right-related data enables the content provider to impose limitations on the usage of the content. The content key is used for decrypting the encrypted content. In case there is another right related to the usage of the content defined by the operator, the priority data is used for defining the priority levels for the right defined by the content provider and the right defined by the operator. In such a way, the content provider can impose limitations on the usage of the content even if the content is delivered by the operator to the end user, and meanwhile, the operator is allowed to
define a personalized usage right for different end users. Both rights defined by the content provider and the operator have been considered and fulfilled.

According to an embodiment of a second aspect of the invention, a method of managing encrypted content by a second device is proposed. Said encrypted content is associated with a first license data, said first license data is received from a first device and comprises a content key for decrypting said encrypted content, and said content key is encrypted with a first key. The method comprises the steps of:

- decrypting said encrypted content key upon receiving a request data from a third device requesting the use of said encrypted content; and

- re-encrypting the content key with a second key associated with said third device so that the re-encrypted content key can be decrypted by said third device.

In such a way, when the third device receives the re-encrypted content key from the operator, the third device is able to decrypt the re-encrypted content key and as a consequence is able to use the content encrypted by the content key. Therefore, the second device can authorize the third device to use the encrypted content and at the same time, the right defined by the first device, i.e. the content provider, can be guaranteed.

Optionally, when the second device, i.e the operator, is not allowed to tamper with the operation of the above two steps, i.e. encrypting and decrypting, in the second device, the right defined by the first device cannot be changed by the second device and the second device cannot get the decrypted content key (clean content key). It means that the above two steps, which are performed on the second device, could be trusted by the content provider. To achieve this purpose, the above two steps can be implemented in a tamper-proof module and the module can be provided by the content provider.

According to an embodiment of a third aspect of the invention, a method of managing encrypted content by a third device is proposed. The method comprises the steps of:

- receiving a license data comprising a first right-related data defining a first right of using said encrypted content and a second right-related data defining a second right of using said encrypted content;

- obtaining a priority data defining the priority levels of the first right and the second right; and
- determining the right of using said encrypted content according to the first right-related data, the second right-related data and the priority data.

By applying the first right-related data determined by the content provider, the second right-related data determined by the operator and the priority data, the user is allowed to use the encrypted content in the way agreed by the content provider and the operator. Therefore, both the right defined by the content provider and the right defined by the operator can be guaranteed.

According to an embodiment of a fourth aspect of the invention, a first device for managing an encrypted content is proposed. The first device comprises:

- a first unit for determining a right-related data and a priority data, said right-related data defining a right of using said encrypted content, said priority data defining the priority level of said right; and
- a second unit for generating a license data for authorizing a second device to use said encrypted content, the license data comprising the right-related data, the priority data and a content key for decrypting said encrypted content.

According to an embodiment of a fifth aspect of the invention, a tamper-proof module for managing encrypted content is proposed. Said content is associated with a first license data, said first license data is received from a first device and comprises a content key for decrypting said encrypted content, said content key being encrypted with a first key. The second device comprises:

- a first unit for decrypting said encrypted content key upon receiving a request data from a third device requesting the use of said encrypted content; and
- a second unit for re-encrypting the content key with a second key associated with said third device so that the re-encrypted content key can be decrypted by said third device.

As described above, the first unit and the second unit are safe, and the tamper-proof module can be provided to the operator by the content provider or a third party trusted by the content provider and then be installed in the second device of the operator.

According to an embodiment of a sixth aspect of the invention, a second device for managing encrypted content is proposed. The second device comprises the above tamper-proof module, wherein said first license data further comprises a first right-related data defining a first right of using said encrypted content, said second device further comprising:
- a third unit for generating a second right-related data defining a second right of using said encrypted content; and

- a fourth unit for generating a second license data comprising the first right-related data, the second right-related data and the re-encrypted content key, said second license data being intended to authorize the third device to use said encrypted content.

According to an embodiment of a seventh aspect of the invention, a third device for managing encrypted content is proposed. The third device comprises:

- a receiver for receiving a license data comprising a first right-related data defining a first right of using said encrypted content and a second right-related data defining a second right of using said encrypted content;

- a first unit for obtaining a priority data defining the priority levels of the first right and the second right, and

- a second unit for determining the right of using said encrypted content according to the first right-related data, the second right-related data and the priority data.

These and other aspects of the invention will be apparent from and elucidated with reference to the embodiments described hereinafter.

DESCRIPTION OF THE DRAWINGS

The above and other objects and features of the present invention will become more apparent from the following detailed description considered in connection with the accompanying drawings, in which:

Fig. 1 depicts a flow chart of the method of managing encrypted content by the first device according to an embodiment of the invention;

Fig. 2 depicts a flow chart of the method of managing encrypted content by the second device according to an embodiment of the invention;

Fig. 3 depicts a flow chart of the method of managing encrypted content by the second device according to another embodiment of the invention;
Fig. 4 depicts a flow chart of the method of managing encrypted content by the third device according to an embodiment of the invention;

Fig. 5 depicts a schematic block diagram of an embodiment of the first device;

Fig. 6 depicts a schematic block diagram of a module of the second device;

Fig. 7 depicts a schematic block diagram of another embodiment of the second device;

Fig. 8 depicts a schematic block diagram of an embodiment of the third device; and

Fig. 9 depicts a schematic block diagram of a system according to an embodiment of the invention.

The same reference numerals are used to denote similar parts throughout the Figures.

DETAILED DESCRIPTION

Fig. 9 depicts a schematic block diagram of a system 900 according to an embodiment of the invention.

Referring to Fig. 9, the system 900 comprises a first device 500, a second device 700 and a third device 800. Encrypted content is transmitted from the first device 500 to the second device 700 and then from the second device 700 to the third device 800.

In an embodiment of the system, the first device 500 can be a device at a content provider side, the second device 700 can be a device at an operator side and the third device 800 can be a device (such as a STB) at an end user side.

In the following description, it is described how to manage the encrypted content transmitted among the first device 500, the second device 700 and the third device 800.

According to an embodiment of a first aspect of the present invention, a method of managing encrypted content performed by the first device 500 is proposed.

Fig. 1 depicts a flow chart of the method of managing encrypted content by the first device 500.

Referring to Fig. 1, the method comprises a step 110 of determining a right-related data and a priority data by the first device 500. The right-related data defines a right of using the encrypted content and the priority data defines the priority level of the right.
The encrypted content could be encrypted by any symmetrical encryption algorithm or asymmetrical encryption algorithm. This invention does not intend to limit the algorithm for encrypting the content.

The right defined by the first device 500 illustrates a usage limitation of the content. In other words, the right defines an authorization for authorizing the other device to use the content in a designated way. The right can comprise many kinds of limitations, such as the content can only be played and cannot be copied, the content cannot be used more than one thousand times or the content can only be used in a predefined period, such as three months.

The priority data can define the priority level of the right. It is assumed that the first device 500 defines a first right via the right-related data which indicates that the content can only be used in a first way; and then the right-related data is transmitted to the second device 700. Later on, the second device 700 needs to distribute the content to a third device 800. For gaining a better interest, according to the business model of the second device 700, the second device 700 may need to define a second right which indicates that the content can only be used in a second way. On the other hand, the first device 500 representing the interest of the content provider needs to protect the content provider's interests by imposing the first right wherever the content is transmitted by the second device 700.

In this context, the priority data actually defines a rule on how to determine the right of using a content according to many different rights in case the license data related to this content comprises many different right-related data defining different rights of using this content. The different rights for example could be defined according to the way of doing business by the content provider and the operator. There are many ways to define this rule.

The right of using the content is determined finally according to the priority data, the first right and the second right. When, for example, the priority data defines that the content should be used according to the second right if the second right and the first right are in conflict, for example, it is allowed to use the content according to the first right data but it is not allowed to use the content according to the second right data. In other example, whether the content is allowed to be used should depend on both the first right data and the second right data in case there is conflict between two rights. For example, according to the first right, the content is only allowed to be played and is not allowed to be copied; however, according to the second right, the
content can be both played and copied. The priority data is very beneficial to solve the conflict between rights.

For solving the conflict between the rights, the rule defined by the priority data could comprise for example that in case of a conflict, the content's usage right should be decided according to the first right data. According to another example of the rule for solving conflicts, the rule could be that the content's usage right should be decided according to the second right data. A third example could be to determine the content's usage right according to the right which indicates a negative result (i.e. the negative result means it is not allowed to use the content or has less usage rights); the rule means that the content cannot be used if any right determines that it is not allowed to use the content, or on the contrary, according to the right which indicates a optimistic result, i.e. the content can be used if any right determines that the usage of the content is allowed. Optionally, the priority data can define that the first right is ignored if the operator has paid an extra fee to the content provider.

When the priority data defines that the right defined by the first device 500 can limit the right defined by the second device 700, the right defined by the first device 500 can be guaranteed, i.e. the interests of the content provider are guaranteed.

For example, the content provider defines a first right that the content can only be used from Jan. 1, 2009 to Jun. 1, 2009 and the operator defines a second right that the content can only be used from Feb. 1, 2009 to Oct. 1, 2009. Because of limitation period of the first right, the content can only be used from Feb. 1 to Jun. 1.

The method further comprises a step 120 of generating, by the first device 500, a license data. The license data comprises the right-related data, the priority data and the content key for decrypting the encrypted content. The license data is intended to authorize the second device to use the encrypted content.

In an embodiment of the method, the first device 500 encrypts the content key with a first key associated with the second device 700 so that the second device 700 can decrypt the encrypted content key. The encrypted content key is comprised in the license data before the license data is transmitted to the second device 700. In this way, the content key can be accessed by an authorized second device 700, but cannot be accessed by an illegal user.
The content key can be encrypted with the first key with symmetric encryption algorithms or asymmetric encryption algorithms. When the content key is encrypted with a symmetric encryption algorithm, the first key is also the decryption key for decrypting the encrypted content key by the second device 700. When the content key is encrypted with an asymmetric encryption algorithm, the first key is the public key of a public/private key pair of the second device 700; and thus, the second device 700 can decrypt the encrypted content key with the private key of the public/private key pair.

To authorize the second device 700 to use the encrypted content, the first device 500 transmits the encrypted content and the license data to the second device 700. The license data has advantages since it comprises not only the traditional item, i.e. right and content key, but also a priority data. By having the priority data in the license data, it is possible for the first device 500 to impose the first right and meanwhile give some freedom to the second device 700 to define a second right according to the operator's interests.

Fig. 2 depicts a flow chart of the method of managing encrypted content by the second device 700 according to an embodiment of the invention.

According to an embodiment of a second aspect of the invention, a method of managing encrypted content performed by the second device 700 is proposed.

Firstly, the second device 700 receives the encrypted content and also receives an associated license data (i.e. the license data described in the embodiments of the method of managing the encrypted content in the first device 500) from the first device 500. The associated license data is intended to be used for authorizing the second device 700 to use and distribute the content. As mentioned above, the license data comprises the content key for decrypting the encrypted content, and the content key is encrypted with the first key. In the following, in order to distinguish it from other license data generated by the second device 700, the license data generated by the first device 500 is referred to as "the first license data"

Referring to Fig. 2, the method comprises a step 210 of decrypting, by the module 600 in the second device 700, the encrypted content key upon receiving a request data from the third device 800 requesting the use of the encrypted content. As mentioned above, since the first key is related to the second device 700, the second device 700 can decrypt the encrypted content key according to the encryption algorithm used for encrypting the content key.
The method further comprises a step 220 of re-encrypting the content key with a second key associated with the third device 800 by the module 600, so that the re-encrypted content key can be decrypted by the third device 800. The module 600 in the second device 700 can re-encrypt the content key with the second key with symmetric encryption algorithms or asymmetric encryption algorithms. Symmetric encryption algorithms or asymmetric encryption algorithms is well known by the skilled person in the field of cryptography. Therefore, it will not be described in details in this application. Similarly to the encryption of the content key with the first key, the algorithm for re-encrypting the content key could either be the symmetric encryption algorithm or the asymmetric encryption algorithm. The second key is associated with the third device 800, for example the public key of a public/private key pair of the third device 800 in case of asymmetric encryption algorithm. Therefore, the third device 800 is able to decrypt the re-encrypted content key.

By decrypting the encrypted content key and re-encrypting the content key with the second key associated with the third device 800, it is possible to authorize the third device 800 to use the content encrypted by the content key. Therefore, the second device 700 can authorize the third device 800 to use the encrypted content.

Optionally, the data requested from the third device 800 can be recorded by the second device 700. It could be used by the second device 700 or the first device 500 to calculate how many requests originate from the end user requesting the content. For example, the number of request data is recorded and the first device 500 can determine whether the content has been transmitted in excess of a limitation, such as ten thousand users, defined in the contract. In another embodiment, based on the recorded result, the second device 700 can determine whether the request from the user should be fulfilled according to the first right or the contract signed between the operator and the content provider. For example, if the content has been requested at a time which is not in a time period defined in the contract, the second device 700 does not decrypt the content key and the user's request cannot be fulfilled.

Fig. 3 depicts a flow chart of the method of managing encrypted content by the second device 700 according to another embodiment of the invention.

The first license data further comprises a first right-related data defining a first right of using the encrypted content. The first right is a limitation on the use of the content and the first
right can be defined by the first device 500. The first right can comprise many kinds of limitations, such as the content can only be played and cannot be copied, the content cannot be used for more than one thousand times or the content can only be used in a predefined time period.

Referring to Fig. 3, the method further comprises a step 310 of generating by the second device 700 a second right-related data defining a second right of using the encrypted content.

The second right is another usage limitation of the content. The second right can comprise many kinds of limitations, such as the content can only be played and cannot be copied, the content can be used only one time or the content can only be used in a predefined time period, such as two days.

Following the step 310, the method further comprises a step 320 of generating by the second device 700 a second license data. The second license data comprises the first right-related data, the second right-related data and the re-encrypted content key. The second license data is intended to authorize the third device 800 to use the encrypted content.

When the first right-related data is determined by the first device 500 and the second right-related data is determined by the second device 700, both the content provider's right and the operator's right can be imposed on the encrypted content.

In an embodiment of the method, since the first license data comprises a priority data defining the priority levels of the first right and the second right, the method further comprises a step of obtaining the priority data from the first license data. And the second license data further comprises the priority data.

It is to be understood that the first device 500 may send a first license data without the priority data. In this case, the method further comprises a step of generating a priority data defining the priority levels of the first right and the second right by the second device 700. And the second license data further comprises the priority data.

How the priority data in the above two embodiments defines the priority levels of the first right and the second right can be found in the corresponding description of the priority data in the embodiment of managing the encrypted content by the first device 500, and is not elaborated here.

In a further embodiment of the method, the second device 700 re-encrypts the encrypted content with a service key, and encrypts the service key with the second key associated with the
third device 800 so that the encrypted service key can be decrypted by the third device 800. The second license data further comprises the encrypted service key. The third device 800 can decrypt the service key, and then decrypt the content, using the service key.

For re-encrypting the encrypted content, any symmetric encryption algorithm or asymmetric encryption algorithm can be used. This invention does not intend to limit the algorithms for re-encrypting the encrypted content.

To authorize the third device 800 to use the encrypted content, the second device 700 transmits the encrypted content and the second license data to the third device 800.

According to an embodiment of a third aspect of the invention, a method of managing encrypted content by the third device 800 is proposed.

Fig. 4 depicts a flow chart of the method of managing encrypted content by the third device 800 according to an embodiment of the invention.

Referring to Fig. 4, the method comprises a step 410 of receiving a license data (i.e. the second license data described in the embodiments of the method of managing the encrypted content in the second device 700) by the third device 800 from the second device 700. The license data comprises: the first right-related data which defines the first right of using the encrypted content, the second right-related data which defines the second right of using the encrypted content and the priority data.

The method further comprises a step 420 of obtaining, by the third device 800, from the second license data, the priority data defining the priority levels of the first right and the second right.

The method further comprises a step 430 of determining, by the third device 800, whether the encrypted content is allowed to be used according to the first right-related data, the second right-related data and the priority data.

The received license data also comprises an encrypted content key for decrypting the encrypted content, and if the determining step 430 indicates that the content is allowed to be used, the method further comprises a step of decrypting the encrypted content key by the third device 800, and a step of decrypting, by the third device 800, the encrypted content with the decrypted content key.
When the content key is encrypted with the second key with symmetric encryption algorithms, the third device 800 can decrypt the content key with the second key stored in the third device 800; when the content key is encrypted with the second key with asymmetric encryption algorithms, the third device 800 can decrypt the content key with the private key of the third device 800.

In another embodiment of the method, the encrypted content is content which is encrypted first with a content key and then with a service key; the license data further comprises an encrypted content key and an encrypted service key for decrypting the encrypted content, and if the determining step 430 indicates that the content is allowed to be used, the method further comprises a step of decrypting, by the third device 800, the encrypted content key and the encrypted service key, and a step of decrypting, by the third device 800, the encrypted content with the decrypted service key and the decrypted content key. The encrypted content is decrypted first with the service key and then with the content key.

Similarly to the content key, when the service key is encrypted with the second key with symmetric encryption algorithms, the third device 800 can decrypt the service key with the second key stored in the third device; when the service key is encrypted with the second key with asymmetric encryption algorithms, the third device 800 can decrypt the service key with a private key stored in the third device 800.

By using the service key, the second device 700 could be used both for dealing with the content transmitted from the first device 500 and for handling the content generated or owned completely by the second device 700; in the latter situation, the content will only be encrypted in the second device 700 with the service key, and the service key is deemed to be the content key for decrypting the content.

Fig. 5 depicts a schematic block diagram of one embodiment of the first device 500.

According to an embodiment of a fourth aspect of the present invention, the first device 500 for managing encrypted content is proposed.

Referring to Fig. 5, the first device 500 comprises a first unit 510 for executing the step 110 described above. The right-related data defines a right of using the encrypted content, and the priority data defines the priority level of the right.
The first device 500 further comprises a second unit 520 for executing the step 120 described above. The license data is intended to authorize the second device 700 to use the encrypted content. The output of the first unit 510 is an input for the second unit 520.

In an embodiment of the first device 500, the first device 500 further comprises a third unit (not shown) for encrypting the content key with a first key associated with the second device 700 so that the second device 700 can decrypt the encrypted content key, wherein the encrypted content key is comprised in the license data.

In another embodiment of the first device 500, the first device 500 further comprises a transmitter (not shown) for transmitting the encrypted content and the license data to the second device 700.

Fig. 6 depicts a schematic block diagram of a module of the second device 700. Fig. 7 depicts a schematic block diagram of another embodiment of the second device 700.

According to an embodiment of a fifth aspect of the present invention, a module 600 for managing encrypted content is proposed. The encrypted content is associated with a first license data, and the first license data is received from a first device 500. The first license data comprises a content key for decrypting the encrypted content, and the content key is encrypted with a first key.

Referring to Fig. 6, the module 600 comprises a first unit 610 for executing the step 210 described above.

The module 600 further comprises a second unit 620 for executing the step 220 described above. The output of the first unit 610 is an input for the second unit 620.

In an embodiment of the second unit 620, the second unit 620 transmits the re-encrypted content key to the other units in the second device 700.

The first unit 610 and the second unit 620 can be integrated to form a module that is to be sold separately. The module 600 can be implemented in many ways, such as a control card that can be inserted into the second device 700, a detachable chipset installed in the second device 700 or a software module implemented entirely by software.

Preferably, the module 600 is tamper-proof. The operation of the first unit 610 and the second unit 620 cannot be tampered with by the operation of the other units in the second device.
700. In this way, the right and the priority data defined by the first device 500 cannot be changed by the operator when using the second device 700. In this way, the content provider can guarantee the content to be used according to the rule defined by the content provider.

Referring to Fig. 7, the second device 700 further comprises a third unit 710 for executing the step 310 described above; and a fourth unit 720 for executing the step 320 described above. The output of the second unit 620 is an input for the fourth unit 720.

In another embodiment of the second device 700, the first license data comprises a priority data defining the priority levels of the first right and the second right, the second device 700 further comprising a fifth unit (not shown) for obtaining the priority data, wherein the second license data further comprises the priority data.

By generating new right data and license data, the benefits of both the content provider and the operator can be guaranteed, and the operator has more flexibility while the right of the content provider is guaranteed.

In a further embodiment of the second device 700, the fourth unit 720 is further adapted to perform the above mentioned step of generating the priority data defining the priority levels of the first right and the second right, the second license data further comprising the priority data.

In a further embodiment of the second device 700, the second device 700 further comprises a sixth unit (not shown) for performing the above mentioned step of recording the request data.

In an embodiment of the second device 700, the second device 700 further comprises a first transmitter (not shown) for transmitting the recorded result recorded by the sixth unit to the first device 500.

In an embodiment of the second device 700, the second device 700 further comprises a second transmitter (not shown) for transmitting the encrypted content and second license data to the third device 800.

It is to be understood that the first and the second transmitter could be the same transmitter.

According to an embodiment of a seventh aspect of the present invention, the third device 800 for managing encrypted content is proposed.

Fig. 8 depicts a schematic diagram of an embodiment of the third device 800.
Referring to Fig. 8, the third device 800 comprises a receiver 810 for executing the step 410 described above.

The third device 800 further comprises a first unit 820 for executing the step 420 described above.

The third device 800 further comprises a second unit 830 for executing the step 430 described above.

In an embodiment of the third device 800, wherein the license data further comprises an encrypted content key for decrypting the encrypted content, and, if the second unit 830 indicates that the encrypted content is allowed to be used, the third device 800 further comprises a third unit (not shown) for decrypting the encrypted content key, and a fourth unit (not shown) for decrypting the encrypted content with the decrypted content key.

In another embodiment of the third device 800, the encrypted content is content which is encrypted first with a content key and then with a service key; the license data further comprises the encrypted content key and the encrypted service key for decrypting the encrypted content, and, if the second unit 830 indicates that the encrypted content is allowed to be used, the third device 800 further comprises a fifth unit (not shown) for decrypting the encrypted content key and the encrypted service key, and a sixth unit (not shown) for decrypting the encrypted content with the decrypted service key and the decrypted content key.

The above mentioned function units in the first, second and third device could be implemented by software, hardware or the combination of software and hardware. For example, they could be implemented by a processor and a memory stored with instruction code or by an integrated chipset, etc.

It should be noted that the above-mentioned embodiments illustrate rather than limit the invention and that those skilled in the art will be able to design alternative embodiments without departing from the scope of the appended claims. In the claims, any reference signs placed between parentheses shall not be construed as limiting the claim. The word "comprising" does not exclude the presence of elements or steps not listed in a claim or in the description. The word "a" or "an" preceding an element does not exclude the presence of a plurality of such elements. In the apparatus claims enumerating several units, several of these units can be embodied by one
and the same item of hardware or software. The usage of the words first, second and third, et cetera, does not indicate any ordering. These words are to be interpreted as names.
CLAIMS:
1. A method of managing encrypted content by a first device, comprising the steps of:
   - determining (110) a right-related data and a priority data, said right-related data defining a right of using said encrypted content, said priority data defining the priority level of said right; and
   - generating (120) a license data for authorizing a second device to use said encrypted content, said license data comprising the right-related data, the priority data and a content key for decrypting said encrypted content.

2. A method of managing encrypted content by a second device, said encrypted content being associated with a first license data, said first license data being received from a first device and comprising a content key for decrypting said encrypted content, said content key being encrypted with a first key, said method comprising the steps of:
   - decrypting (210) said encrypted content key upon receiving a request data from a third device requesting the use of said encrypted content; and
   - re-encrypting (220) the content key with a second key associated with said third device so that the re-encrypted content key can be decrypted by said third device.

3. A method as claimed in claim 2, said first license data further comprising a first right-related data defining a first right of using said encrypted content, said method further comprising the steps of:
   - generating (310) a second right-related data defining a second right of using said encrypted content; and
   - generating (320) a second license data for authorizing the third device to use said encrypted content, said second license data comprising the first right-related data, the second right-related data and the re-encrypted content key.

4. A method as claimed in claim 3, said first license data comprising a priority data defining the priority levels of the first right and the second right, the method further comprising a step of:
- obtaining said priority data from the first license data, wherein said generated second license data further comprises said priority data.

5. A method as claimed in claim 3, further comprising a step of:
   - generating by said second device, a priority data defining the priority levels of the first right and the second right, said generated second license data further comprising said priority data.

6. A method as claimed in claim 2, further comprising a step of recording said request data.

7. A method of managing encrypted content by a third device, comprising the steps of:
   - receiving (410) a license data comprising a first right-related data defining a first right of using said encrypted content and a second right-related data defining a second right of using said encrypted content;
   - obtaining (420) a priority data defining the priority levels of the first right and the second right; and
   - determining (430) the right of using said encrypted content according to the first right-related data, the second right-related data and the priority data.

8. A first device for managing encrypted content, comprising
   - a first unit (510) for determining a right-related data and a priority data, said right-related data defining a right of using said encrypted content, said priority data defining the priority level of said right; and
   - a second unit (520) for generating a license data for authorizing a second device to use said encrypted content, said license data comprising the right-related data, the priority data and a content key for decrypting said encrypted content.

9. A tamper-proof module (600) for managing encrypted content, said encrypted content being associated with a first license data, said first license data being received from a first device and comprising a content key for decrypting said encrypted content, said content key being encrypted with a first key, said module comprising:
- a first unit (610) for decrypting said encrypted content key upon receiving a request data from a third device requesting the use of said encrypted content; and
- a second unit (620) for re-encrypting the content key with a second key associated with said third device so that the re-encrypted content key can be decrypted by said third device.

10. A second device for managing encrypted content, comprising the tamper-proof module as claimed in claim 9, wherein said first license data further comprises a first right-related data defining a first right of using said encrypted content, said second device further comprising:
- a third unit (710) for generating a second right-related data defining a second right of using said encrypted content; and
- a fourth unit (720) for generating a second license data comprising the first right-related data, the second right-related data and the re-encrypted content key, said second license data being intended to authorize the third device to use said encrypted content.

11. A second device as claimed in claim 10, said first license data comprising a priority data defining the priority levels of the first right and the second right, said second device further comprising:
- a fifth unit for obtaining said priority data, wherein said generated second license data further comprises said priority data.

12. A second device as claimed in claim 10, wherein the fourth unit (720) is further adapted to generate a priority data for defining the priority levels of the first right and the second right, said generated second license data further comprising said priority data.

13. A second device as claimed in claim 10, further comprising a sixth unit for recording said request data.

14. A third device for managing encrypted content, comprising:
- a receiver (810) for receiving a license data comprising a first right-related data defining a first right of using said encrypted content and a second right-related data defining a second right of using said encrypted content;

- a first unit (820) for obtaining a priority data defining the priority levels of the first right and the second right, and

- a second unit (830) for determining the right of using said encrypted content according to the first right-related data, the second right-related data and the priority data.

15. A third device as claimed in claim 14, wherein said license data further comprises an encrypted content key for decrypting the encrypted content, and, if the second unit (830) indicates that the encrypted content is allowed to be used, the third device further comprises:

- a third unit for decrypting the encrypted content key; and

- a fourth unit for decrypting the encrypted content with the decrypted content key.
A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/00
ADD.
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED
Minimum documentation searched (classification system followed by classification symbols)
G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>US 5 982 891 A (GINTER KARL L [US] ET AL) 9 November 1999 (1999-11-09) figures 2,2a</td>
</tr>
<tr>
<td>A</td>
<td>WO 02/067548 A1 (RPK NEW ZEALAND LTD [NZ]; RAIKE WILLIAM MICHAEL [NZ]; DONOVAN-SMITH BR) 29 August 2002 (2002-08-29) * abstract</td>
</tr>
</tbody>
</table>

Further documents are listed in the continuation of Box C. See patent family annex.

Special categories of cited documents:

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

Date of the actual completion of the international search
13 December 2010

Date of mailing of the international search report
30/12/2010

Name and mailing address of the ISA/
European Patent Office, P.B. 5818 Patentpan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer
Kerschbaumer, J
<table>
<thead>
<tr>
<th>Patent document cited in search report</th>
<th>Publication date</th>
<th>Patent family member(s)</th>
<th>Publication date</th>
</tr>
</thead>
<tbody>
<tr>
<td>US 2004184616 A1</td>
<td>23-09-2004</td>
<td>CA 2559323 A1</td>
<td>30-09-2004</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CN 1761948 A</td>
<td>19-04-2006</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 1606715 A2</td>
<td>21-12-2005</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 2006524007 T</td>
<td>19-10-2006</td>
</tr>
<tr>
<td></td>
<td></td>
<td>KR 20050119122 A</td>
<td>20-12-2005</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2006101287 A1</td>
<td>11-05-2006</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NO 2004084035 A2</td>
<td>30-09-2004</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AT 441897 T</td>
<td>15-09-2009</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AT 412945 T</td>
<td>15-11-2008</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AU 711733 B2</td>
<td>21-10-1999</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CA 2212574 A1</td>
<td>06-09-1996</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CA 2683230 A1</td>
<td>06-09-1996</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CN 1601429 A</td>
<td>30-03-2005</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CN 1183841 A</td>
<td>03-06-1998</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CN 1577205 A</td>
<td>09-02-2005</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CN 1722049 A</td>
<td>18-01-2006</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CN 1869997 A</td>
<td>29-11-2006</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CN 1900942 A</td>
<td>24-01-2007</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CN 1912885 A</td>
<td>14-02-2007</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CN 1936912 A</td>
<td>28-03-2007</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CN 1900943 A</td>
<td>24-01-2007</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CN 101398871 A</td>
<td>01-04-2009</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CN 101359350 A</td>
<td>04-02-2009</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CN 101303717 A</td>
<td>12-11-2008</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 1431864 A2</td>
<td>23-06-2004</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 1515216 A2</td>
<td>16-03-2005</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 1531379 A2</td>
<td>18-05-2005</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 1526472 A2</td>
<td>27-04-2005</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 1555591 A2</td>
<td>20-07-2005</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 1643340 A2</td>
<td>05-04-2006</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 1662418 A2</td>
<td>31-05-2006</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 1923814 A2</td>
<td>21-05-2008</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 2015214 A2</td>
<td>14-01-2009</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 2110732 A2</td>
<td>21-10-2009</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 0861461 A2</td>
<td>02-09-1998</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HK 1073899 A1</td>
<td>07-12-2007</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HK 1085824 A1</td>
<td>28-11-2008</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HK 1099380 A1</td>
<td>09-04-2010</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HK 1099098 A1</td>
<td>18-09-2009</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HK 1102199 A1</td>
<td>18-09-2009</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 10512074 T</td>
<td>17-11-1998</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 3996532 B2</td>
<td>24-10-2007</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 2004265358 A</td>
<td>24-09-2004</td>
</tr>
<tr>
<td>US 5982891 A</td>
<td></td>
<td>JP 2004005558 A</td>
<td>08-01-2004</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 2004005601 A</td>
<td>08-01-2004</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 2004139550 A</td>
<td>13-05-2004</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 2004030600 A</td>
<td>29-01-2004</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 2004005614 A</td>
<td>08-01-2004</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 4128902 B2</td>
<td>30-07-2008</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 2004005625 A</td>
<td>08-01-2004</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 2004005629 A</td>
<td>08-01-2004</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 4272129 B2</td>
<td>03-06-2009</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 2006073004 A</td>
<td>16-03-2006</td>
</tr>
<tr>
<td>Patent document cited in search report</td>
<td>Publication date</td>
<td>Patent family member(s)</td>
<td>Publication date</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-----------------</td>
<td>-------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>US 2004249768 A1</td>
<td>09-12-2004</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE 60210938 T2</td>
<td>16-11-2006</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 1371170 A1</td>
<td>17-12-2003</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 2004529534 T</td>
<td>24-09-2004</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 2008252956 A</td>
<td>16-10-2008</td>
</tr>
</tbody>
</table>