(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 May 2012 (03.05.2012)

PCT

(10) International Publication Number
WO 2012/057577 A2

(51) International Patent Classification:
*G06F 21/20* (2006.01)

(21) International Application Number:
PCT/KR2011/008160

(22) International Filing Date:
28 October 2011 (28.10.2011)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10-2010-0107317 29 October 2010 (29.10.2010) KR

(71) Applicant *(for all designated States except US)*: **SAMSUNG ELECTRONICS CO., LTD.** [KR/KR]; 416, Maetan-dong, Yeongtong-gu, Suwon-si, Gyeonggi-do 442-742 (KR).

(72) Inventors: **KANG, Bo-Gyeong**; #1-607, Limkwang APT., Maetan 3-dong, Suwon-si, Gyeonggi-do 443-714 (KR). **LEE, Byung-Rae**; #1115, Raemian Seocho Univille, Seocho 1-dong, Seocho-gu, Seoul 137-918 (KR).

(74) Agent: **LEE, Keon-Joo**; Mihwa Bldg. 110-2, Myongryun-dong 4-ga, Chongro-gu, Seoul 110-524 (KR).

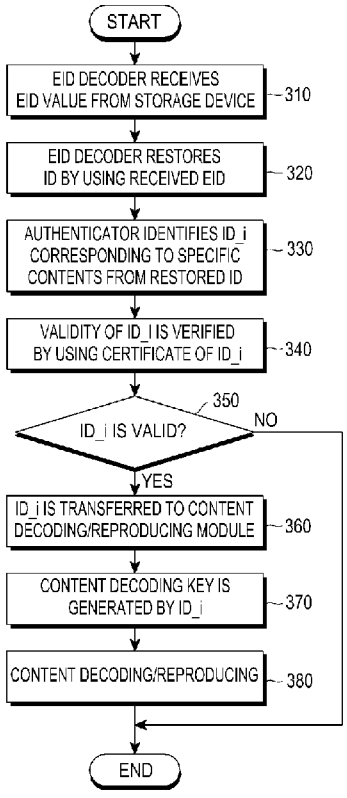
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

*[Continued on next page]*

WO 2012/057577 A2

(54) Title: STORAGE DEVICE, AND AUTHENTICATION METHOD AND AUTHENTICATION DEVICE OF STORAGE DEVICE

[Fig. 3]




(57) Abstract: An authentication method of a storage device includes requesting an EID (Encoded IDentifer) to the storage device by an authentication device for authenticating the storage device, receiving the EID by the authentication device, restoring original ID information by decoding the received EID, and verifying individual ID information corresponding to use of the storage device included in ID information by using ID authentication information received from the storage device, wherein the ID information includes multiple pieces of individual ID information corresponding to the use of the storage device.

(84) **Designated States** *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

**Published**:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

# Description

# Title of Invention: STORAGE DEVICE, AND AUTHENTICATION METHOD AND AUTHENTICATION DEVICE OF STORAGE DEVICE

## Technical Field

[1] The present invention relates generally to a non-volatile storage device, and more particularly, to an authentication method and an authentication device of the non-volatile storage device.

## Background Art

[2] In DRM (Digital Rights Management) technology, CPRM (Content Protection for Recordable Media) technology for an SD (Secure Digital) card, and an AACS (Advanced Access Content System) technology for a blue-ray disc, authentication of a storage device is performed by using a cryptographic technology such as a PKI (Public Key Infrastructure).

[3] A storage device uses a specific identifier regardless of the use for its own security. When a storage device is deemed as an inappropriate storage medium by an authentication process as described above, a corresponding storage device is discarded through a separate process.

[4] In a device authentication method of a CPRM technology for an SD card, and an AACS technology for a blu-ray disc, an identifier is stored at a position appointed as a read-only area when the storage medium is produced, and a cryptographic scheme is employed for device authentication and content protection.

## Disclosure of Invention

## Technical Problem

[5] However, after the production, if the identifier is discarded due to any illegal use of the storage device, the storage device (i.e., SD card, Blue-ray disk) may no longer be used for any purpose.

[6] Accordingly, there is a need in the art for a method for providing identifiers according to various uses of a storage device.

## Solution to Problem

[7] Accordingly, an aspect of the present invention is to solve the abovestated problems occurring in the prior art, and to provide a storage device, and an authentication method and an authentication device of the storage device, in which identifiers are provided according to uses of the storage device so that authentication can be individually performed for each identifier.

[8] In accordance with the present invention, there is provided an authentication method of a storage device, including requesting an EID (Encoded IDentifier) to the storage device by an authentication device for authenticating the storage device, receiving the EID from the storage device by the authentication device in accordance with the request, restoring original ID information by decoding the received EID, and verifying individual ID information corresponding to use of the storage device included in ID information by using ID authentication information received from the storage device, wherein the ID information includes multiple pieces of individual ID information corresponding to the use of the storage device.

[9] In accordance with the present invention, there is provided an authentication device for authenticating a storage device, the authentication device including an ID decoder for requesting an EID to the storage device, receiving the EID from the storage device in accordance with the request, and restoring original ID information by decoding the received EID, and an authenticator for verifying individual ID information corresponding to use of the storage device included in ID information by using ID authentication information received from the storage device, wherein the ID information includes multiple pieces of individual ID information corresponding to the use of the storage device.

[10] In accordance with the present invention, there is provided a storage device including: an EID area which is positioned at a particular area of the storage device, and stores an EID for specifically identifying the storage device, and ID authentication information including information for verifying ID information, wherein the ID information includes multiple pieces of individual ID information corresponding to use of the storage device.

## Advantageous Effects of Invention

[11] In the present invention, various identifiers are provided according to uses of the storage device, and each identifier is individually authenticated. Accordingly, when authentication on an identifier for a specific use of the storage device fails, it is possible to individually discard only the function of the authentication-failed specific use, instead of the entire storage device. Accordingly, even though a function for a specific use of the storage device is discarded, the storage device can be continuously utilized for other uses, thereby improving the applicability of the storage device. Also, the storage device of the present invention can perform an authentication process on various identifiers by using the same authentication device (ID decoder) in the same manner.

## Brief Description of Drawings

[12] The above and other aspects, features and advantages of the present invention will be

more apparent from the following detailed description taken in conjunction with the accompanying drawings, in which:

[13] FIG. 1 illustrates the structure of an identifier, and the configuration of a storage device, according to the present invention;

[14] FIG. 2 illustrates the configuration of an authentication device performing authentication of a storage device, according to the present invention; and

[15] FIG. 3 illustrates an authentication process of a storage device, according to the present invention.

## Mode for the Invention

[16] Hereinafter, a device and an operation of the present invention will be described in detail with reference to the accompanying drawings. In the following description, specific details such as configuration elements are set forth in order to provide a thorough understanding of the present invention. It will be apparent to those skilled in the art that various changes and modifications can be made without departing from the spirit of the present invention. Also, well known technologies will not be described in detail herein for the sake of clarity and conciseness.

[17] The present invention discloses an individual authentication method and a device thereof according to the use of a non-volatile storage device, which can improve the applicability of the storage device. To this end, the storage device of the present invention includes a plurality of IDs corresponding to respective functions of the storage device at a specific area, in which the IDs are encoded. When the storage device is used, the authentication device for authenticating the storage device restores an original ID by using an ID decoder, and performs an authentication by verifying an ID corresponding to the use. When the authentication of a storage device fails due to a particular illegal use of the storage device, only an ID corresponding to the particular illegal use of the ID is discarded so as to inhibit the illegal use. Accordingly, the storage device may be continuously utilized for other purposes.

[18] FIG. 1 illustrates the structure of an identifier, and the configuration of a storage device, according to the present invention.

[19] In FIG. 1, an ID 110 for identifying a storage device 130 includes a plurality of individual IDs (ID_i) and checksums. The individual IDs (ID_i) of the identifier are used to identify respective uses of the storage device. The storage device may be used for various purposes, such as private information storage, data storage using a document encryption technology such as DRM, certificate information storage and content storage. Individual IDs may be generated according to each use.

[20] Referring to FIG. 1, an ID encoder 120 generates an EID by using the ID 110 for identifying the storage device 130.

[21] The storage device 130 includes the EID 131 and certificates 132 corresponding to the respective individual IDs of the ID 110. The certificates 132 correspond to information used to verify the suitability of the ID restored by the authentication device authenticating the storage device.

[22] The ID 110 for identifying the storage device 130 is encoded and converted into the EID 131 through the ID encoder 120 in the generation step or the test step of the storage device 130, and the EID 131 is programmed into the storage device 130. During recording or reproducing of the storage device 130, a host device performing the recording or the reproducing performs authentication of the storage device by using the EID.

[23] FIG. 2 illustrates the configuration of an authentication device performing authentication of a storage device, according to the present invention.

[24] Referring to FIG. 2, the storage device 130 includes the EID 131 for storing encoded ID information, and a plurality of certificates 132 for verifying individual IDs, and may store data such as image contents 133 such as movies, and private information 134. The storage device 130 further includes a controller (not shown) for controlling input/output of the storage device, and reading/writing. The controller controlls the EID and the ID authentication information to be transferred to a authentication device, for authenticating the storage device.

[25] In FIG. 2, an authentication device (host device) 140 for authenticating the storage device 130 includes an EID decoder 141, an authenticator 142, and a content decoding/reproducing module 143.

[26] The EID decoder 141 receives an EID from the storage device 130 and restores an original ID from the EID.

[27] The authenticator 142 receives the ID of the storage device 130 output from the EID decoder 141, and performs authentication of the storage device by performing cryptographic verification. The authentication device 140, that is, the host device, in accordance with the use of the storage device to be used by the host device, determines the legality of the storage device 130 by using an individual ID_i and a certificate 132 of a corresponding storage device.

[28] When an individual ID is determined to be legal by the authenticator 142, the content decoding/reproducing module 143 generates a content decoding key by using the value of the individual ID, and performs content reproduction by decoding contents.

[29] During authentication of the storage device 130, the EID decoder 141 receives an EID from the EID area 131 of the storage device 130, and the authenticator 142 receives a certificate 132 from the storage device.

[30] In order to verify an individual ID of the storage device 130, a Public Key Infrastructure (PKI) using a certificate 132 is used. However, the present invention is not

limited thereto. If a broadcast key management is used, a set of keys capable of key management according to respective uses may be provided instead of the certificate 132. Also, the PKI scheme may be used in combination with a Broadcast Key Management technique. In this case, the storage device 130 may include both a certificate and a set of keys capable of key management.

[31] FIG. 3 illustrates an authentication process of a storage device, according to the present invention.

[32] Referring to FIG. 3, when the host device for performing recording or reproduction of the storage device 130 receives an access request on specific contents of the storage device 130, the authentication device 140 for authenticating the storage device 130 included in the host device makes a request for an EID to the storage device 130 through the EID decoder 141 in step 310, and receives an EID from the storage device 130 according to the request.

[33] The ID decoder 141 may be set to receive only an encoded individual ID ID_i corresponding to the use of the storage device 130, from among EIDs, from the storage device 130 in accordance with the use of the storage device 130. Specifically, when making a request for an EID to the storage device 130, the ID decoder 141 transfers information on the use of the storage device 130.

[34] Based on the information on the use of the storage device according to controller's controlling, the storage device 130 extracts only an encoded individual ID corresponding to the use from the EID 131, and transfers the extracted encoded individual ID to the ID decoder 141.

[35] The ID decoder 141 may be set to receive all of EIDs of the storage device 130 in step 310, and to use only an individual ID corresponding to the use of the storage device 130 in a later step.

[36] In step 320, the EID decoder 141 restores an original ID by using the received EID.

[37] In step 330, the authenticator 142 identifies an individual ID_i corresponding to the use (specific contents) of the storage device from the restored ID. The authenticator 142 receives the certificate 132 corresponding to the individual ID from the storage device.

[38] In step 340, the authenticator 142 verifies the validity of the individual ID ID_i by using the certificate 132. In this validity verification, an algorithm 1 below may be used, as follows.

[39] Hash(ID_i)=?checksum .....algorithm 1

[40] In step 350, it is determined whether the validity of an individual ID has been verified. When the individual ID has been determined to be illegal, the process is ended. The host device may stop the reproduction of contents, and may connect to a predetermined License Authority Site and make a request for discarding of the use of

the corresponding storage device 130 to the connected site by transmitting the reason for the discard.

[41] In step 350, when the individual ID has been determined to be legal, the process proceeds to step 360, in which the content decoding/reproducing module 143 is paged and the individual ID ID_i is transferred to the content decoding/reproducing module 143.

[42] In step 370, when the verified individual ID is defined as an ID for image data, the content decoding/reproducing module 143 generates a content decoding key by using the individual ID. Herein, the content decoding key may be generated by using algorithm 2 as defined below.

[43] Hash(ID_i, Decryption Key)=ContentsDecryptionKey) ..algorithm 2

[44] In step 380, contents are decoded and reproduced.

[45] In the present invention, various identifiers are provided according to uses of the storage device, and each identifier is individually authenticated. Accordingly, when authentication on an identifier for a specific use of the storage device fails, it is possible to individually discard only the function of the authentication-failed specific use, instead of the entire storage device. Accordingly, even though a function for a specific use of the storage device is discarded, the storage device can be continuously utilized for other uses, thereby improving the applicability of the storage device. Also, the storage device of the present invention can perform an authentication process on various identifiers by using the same authentication device (ID decoder) in the same manner.

[46] While the present invention has been described in detail, the embodiments in the description of the present invention are merely an example and the present invention is not limited thereto. It will be understood by those skilled in the art that various changes in form and details may be made therein without departing from the spirit and scope of the invention as defined by the appended claims.

# Claims

[Claim 1] An authentication method of a storage device, the authentication method comprising:
requesting an EID (Encoded IDentifier) to the storage device by an authentication device, for authenticating the storage device;
receiving the EID from the storage device by the authentication device in accordance with the request;
restoring original ID information by decoding the received EID; and
verifying individual ID information corresponding to use of the storage device included in ID information by using ID authentication information received from the storage device,
wherein the ID information includes multiple pieces of individual ID information corresponding to the use of the storage device.

[Claim 2] The authentication method as claimed in claim 1, further comprising determining whether to discard the individual ID information when verification of the individual ID information corresponding to the use of the storage device fails.

[Claim 3] The authentication method of the storage device, as claimed in claim 1, wherein the EID indicates the use of the storage device .

[Claim 4] The authentication method of the storage device, as claimed in claim 1, wherein the verifying of the individual ID information further comprises:
identifying the individual ID information according to the use of the storage device from the restored ID information; and
verifying the individual ID information corresponding to the use of the storage device by using the ID authentication information received from the storage device.

[Claim 5] The authentication method of the storage device, as claimed in claim 1, wherein the individual ID information corresponding to the use of the storage device is verified by using certificate information according to a PKI (Public Key Infrastructure) received from the storage device as the ID authentication information.

[Claim 6] The authentication method of the storage device, as claimed in claim 1, wherein the individual ID information corresponding to the use of the storage device is verified by using, as the ID authentication information, a set of keys that are received from the storage device and are capable of key management according to broadcast key

management.

[Claim 7] An authentication device for authenticating a storage device, the authentication device comprising:
an ID decoder for requesting an EID (Encoded IDentifier) to the storage device, receiving the EID from the storage device in accordance with the request, and restoring original ID information by decoding the received EID; and
an authenticator for verifying individual ID information corresponding to use of the storage device included in ID information by using ID authentication information received from the storage device,
wherein the ID information includes multiple pieces of individual ID information corresponding to the use of the storage device.

[Claim 8] The authentication device as claimed in claim 7, wherein the authentication device determines whether to discard the individual ID information when verification of the individual ID information corresponding to the use of the storage device fails.

[Claim 9] The authentication device as claimed in claim 7, wherein the EID indicates the use of the storage device .

[Claim 10] The authentication device as claimed in claim 7, wherein when the authenticator verifies the individual ID information, the authenticator identifies the individual ID information according to the use of the storage device in the restored ID information and then verifies the individual ID information corresponding to the use of the storage device by using the ID authentication information received from the storage device.

[Claim 11] The authentication device as claimed in claim 7, wherein when the authenticator verifies the individual ID information corresponding to the use of the storage device by using certificate information according to a PKI (Public Key Infrastructure) received from the storage device as the ID authentication information.

[Claim 12] The authentication device as claimed in claim 7, wherein when the authenticator verifies the individual ID information corresponding to the use of the storage device by using, as the ID authentication information, a set of keys that are received from the storage device and are capable of key management according to broadcast key management.

[Claim 13] A storage device comprising:
an EID (Encoded IDentifier) area which is positioned at a particular area of the storage device, and stores an EID for specifically identifying

the storage device; and

ID authentication information including information for verifying ID information; and

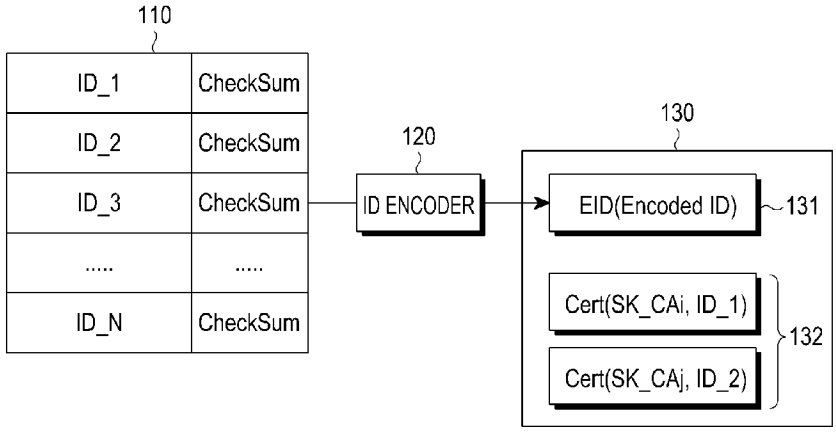
A controller for controlling the EID and the ID authentication information to be transferred to a authentication device for authenticating the storage device,

wherein the ID information includes multiple pieces of individual ID information corresponding to use of the storage device.

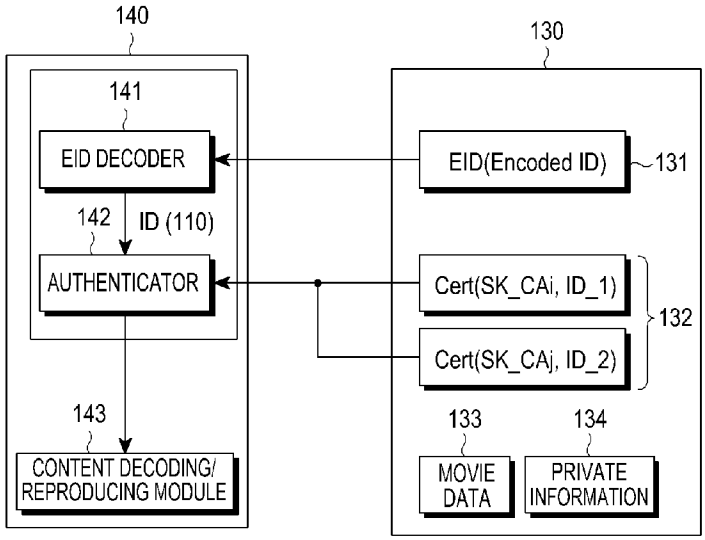
[Claim 14] The storage device as claimed in claim 13, wherein the ID authentication information includes certificate information according to PKI (Public Key Infrastructure).

[Claim 15] The storage device as claimed in claim 13, wherein the ID authentication information includes a set of keys capable of key management according to broadcast key management.

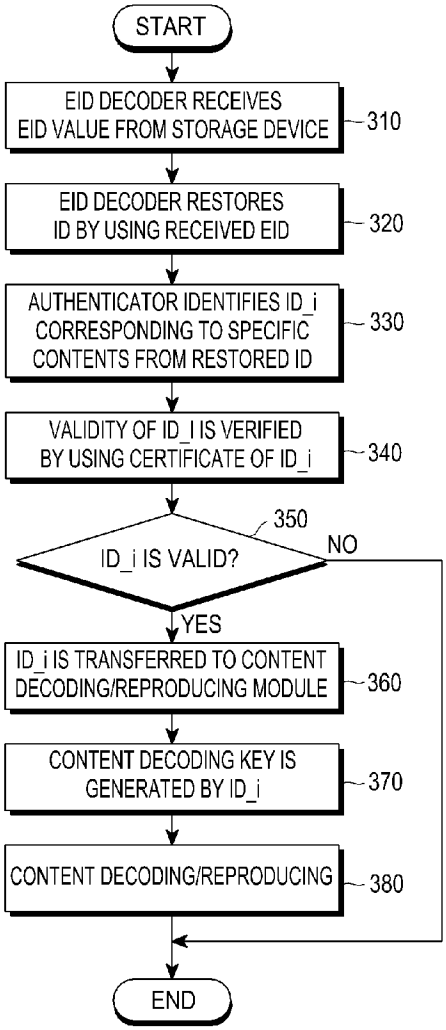
[Fig. 1]


110
ID_1
CheckSum
ID_2
CheckSum
ID_3
CheckSum
.....
.....
ID_N
CheckSum
120
ID ENCODER
130
EID(Encoded ID)
131
Cert(SK_CAi, ID_1)
Cert(SK_CAj, ID_2)
132

[Fig. 2]


140
141
EID DECODER
142
ID (110)
AUTHENTICATOR
143
CONTENT DECODING/
REPRODUCING MODULE
130
EID(Encoded ID)
131
Cert(SK_CAi, ID_1)
Cert(SK_CAj, ID_2)
132
133
MOVIE
DATA
134
PRIVATE
INFORMATION

[Fig. 3]


START
EID DECODER RECEIVES EID VALUE FROM STORAGE DEVICE
310
EID DECODER RESTORES ID BY USING RECEIVED EID
320
AUTHENTICATOR IDENTIFIES ID_i CORRESPONDING TO SPECIFIC CONTENTS FROM RESTORED ID
330
VALIDITY OF ID_I IS VERIFIED BY USING CERTIFICATE OF ID_i
340
350
ID_i IS VALID?
NO
YES
ID_i IS TRANSFERRED TO CONTENT DECODING/REPRODUCING MODULE
360
CONTENT DECODING KEY IS GENERATED BY ID_i
370
CONTENT DECODING/REPRODUCING
380
END