

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
22 June 2006 (22.06.2006)

PCT

(10) International Publication Number
WO 2006/065633 A2

(51) International Patent Classification:
G06F 9/00 (2006.01)

(21) International Application Number:
PCT/US2005/044532

(22) International Filing Date:
8 December 2005 (08.12.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
200410082162.0
17 December 2004 (17.12.2004) CN

(71) Applicant (for all designated States except US): **MO-TOROLA INC.** [US/US]; 1303 East Algonquin Road, Schaumburg, Illinois 60196 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **GAO, Yan** [CN/CN]; Dacheng Nanli 2 Qu 5-3-1101, Beijing, 100039 Beijing (CN). **ZHU, Yu** [CN/CN]; No. 8 Building Jin Song Nan Road Chao, Beijing, 10021 Beijing (CN).

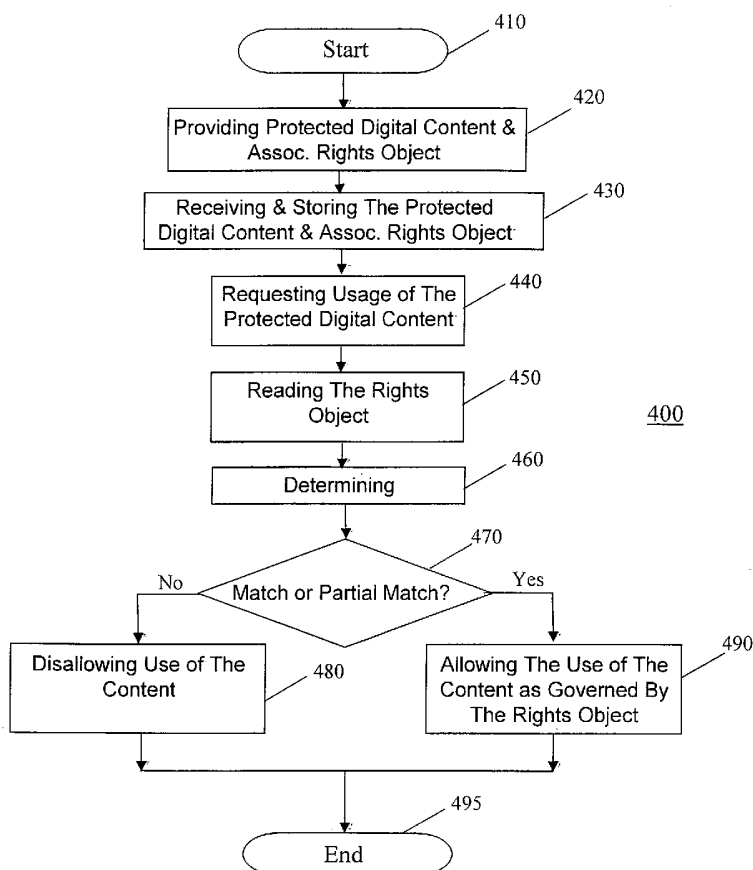
(74) Agents: **VAAS, Randall S.** et al.; 600 North Us Highway 45, Libertyville, Illinois 60048 (US).

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

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: METHOD AND DEVICE FOR DIGITAL RIGHTS MANAGEMENT



(57) Abstract: A method (400) for Digital Rights management (DRM) of protected digital content. The method (400) performs requesting usage of protected digital content (310) to be used by an application supported by an electronics device (100) having a device identity and then reading a rights object (450) associated with and governing allowed use of the protected digital content. Next, the method (400) performs determining from the rights object (460) an identifier and at least one partial match identifier constraint. Thereafter, a decision (470) is provided for allowing (490) the use, governed by the rights object, of the protected digital content by the device (100) only when the device identity exactly matches the identifier or partially matches the identifier as stipulated by the at least one partial match identifier constraint.



Published:

— without international search report and to be republished
upon receipt of that report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

METHOD AND DEVICE FOR DIGITAL RIGHTS MANAGEMENT

Field of the Invention

5

The present invention relates generally to Digital Rights Management (DRM) and in particular, but not necessarily limited to, a method and a device associated with DRM that allows for group access of protected digital content.

10

Background of the Invention

Electronic devices equipped with microprocessors and communication capabilities are becoming more widespread and many new applications are being developed for these devices. Communicating electronic devices are being used to handle digital content such as music, games, video clips, pictures, books; sensitive private data, such as medical records, financial data, credit card numbers; and security and safety situations, such as industrial controls, building automation, security alarms plus other content.

20

In many situations, the digital content, information transferred or sent to these devices needs to be protected at all times. For example, content owners require content rendering devices to be trusted to protect their copyrighted works or content so that access and use of the content can be restricted. Digital content has an intrinsic value and content owners require that protection means be used to ensure that they are fairly compensated for the use of their assets. DRM includes permissions and constraints used to protect rights related to accessing and processing digital content. Content owners hope to protect their valuable digital content using DRM that is implemented by secure, tamper-resistant electronic devices, such as cellular phones.

30

The transfer of protected digital content can be via a peer-to-peer network or by a broadcast of a service provider to a group of devices or by a content provider

allowing content access to one or more devices or by any other method or combination of devices. However, current DRM schemas and methods and devices do not allow use of protected digital content by a group unless each member the group obtains permission to use the content by listing each unique identifier in a rights object provided by a licensed provider or copyright owner of the content.

In this specification, including the claims, the terms 'comprises', 'comprising', 'including' or similar terms are intended to mean a non-exclusive inclusion, such that a method or apparatus that comprises a list of elements does not include those elements solely, but may well include other elements not listed.

Brief Description of the Drawings

In order that the present invention may be readily understood and put into practical affect, reference will now be made to an exemplary embodiment illustrated in the accompanying drawings in which:

FIG. 1 is a block diagram illustrating circuitry of a mobile telephone in accordance with the present invention;

FIG. 2 is a detailed block diagram of a communication system that typically includes a plurality of mobile telephones as illustrated FIG. 1;

FIG. 3 is a conceptual block diagram of what is stored in a static memory of the mobile telephones as illustrated FIG. 1; and

FIG. 4 is a flow chart showing a method of operation of providing and using protected digital content according to an exemplary embodiment of the present invention.

Summary of The Invention

According to one aspect of the invention, there is provided a method for DRM of protected digital content, the method including:

Requesting usage of protected digital content to be used by an application supported by an electronics device having a device identity associated therewith;

reading a rights object associated with and governing allowed use of the protected digital content;

5 Determining from the rights object an identifier and at least one partial match identifier constraint; and

Allowing the use, governed by the rights object, of the protected digital content by the device only when the device identity exactly matches the identifier or partially matches the identifier as stipulated by the at least one partial match identifier
10 constraint.

Suitably, the identifier may be a user identifier identifying a user of the device. One suitable identifier is an identifier of an RUIM or SIM or USIM. Typically, the identifier may be an International Mobile Subscriber Identity or an
15 International Mobile Equipment Identity number.

The identifier may be a telephone number corresponding to an International Mobile Subscriber Identity.

20 Suitably, the least one partial match identifier constraint may be adjacent bits in the International Mobile Subscriber Identity. The adjacent bits may be adjacent least significant bits or an adjacent most significant bits. The adjacent bits may identify a networks provider, or may identify a country, region, state or city. The least one partial match identifier constraint may suitably include matching from one
25 or more of the following: a 10 most significant bits of the identifier; 10 least significant bits of the identifier; n adjacent bits of the identifier; n adjacent bits i bits from the least significant bit of the identifier; n adjacent bits i bits from the most significant bit of the identifier 11th and 12th least significant bits of the identifier; or 11th to 15th least significant bits of the identifier, wherein n and i are integers. Each
30 partial match identifier constraint is allowed to be a combined with one or more other partial match identifier constraints by Boolean operators.

According to another aspect of the invention, there is provided a device comprising:

a memory storing both a protected digital content file and associated object rights, the object rights having an identifier and at least one partial match identifier constraint;

a processor operatively coupled to the memory,

at least one user interface and a keypad operatively coupled to the processor, wherein in response to a user command provided at the keypad the device determines from the rights object an identifier and at least one partial match identifier constraint, and thereafter allows the use by the user interface, governed by the rights object, of the protected digital content by the device only when a device identity that identifies the device exactly matches the identifier or partially matches the identifier as stipulated by the at least one partial match identifier constraint.

Suitably, the identifier may be a user identifier identifying a user of the device. One suitable identifier is a user identifier of an RUIM or SIM or USIM. The identifier may be an International Mobile Subscriber Identity or an International Mobile Equipment Identity number. The identifier may be a telephone number corresponding to an International Mobile Subscriber Identity.

According to another aspect of the invention there is provided a method for providing protected digital content, the method including:

Obtaining a device identity from a device to which the protected digital content is to be provided; and

Providing the protected digital content and an associated rights object, wherein the rights object contains an identifier obtained from the device identity and at least one partial match identifier constraint.

Suitably, the identifier may be a user identifier identifying a user of the device. One suitable identifier is a user identifier of an RUIM or SIM or USIM. The identifier may be an International Mobile Subscriber Identity or an International

Mobile Equipment Identity number. The identifier may be a telephone number corresponding to an International Mobile Subscriber Identity.

Suitably, the least one partial match identifier constraint may be adjacent bits
5 in the telephone number corresponding to an International Mobile Subscriber Identity. The adjacent bits may be adjacent least significant bits or an adjacent most significant bits. The adjacent bits may identify a networks provider, or may identify a country, region, state or city. The least one partial match identifier constraint may suitably include matching from one or more of the following: a 10 most significant
10 bits of the identifier; 10 least significant bits of the identifier; n adjacent bits of the identifier; n adjacent bits i bits from the least significant bit of the identifier; n adjacent bits i bits from the most significant bit of the identifier 11th and 12th least significant bits of the identifier; or 11th to 15^h least significant bits of the identifier, wherein n and i are integers. Each partial match identifier constraint is allowed to be
15 a combined with one or more other partial match identifier constraints by Boolean operators.

Detailed Description of the Drawings

20 The instant disclosure is provided to further explain in an enabling fashion the best mode of making and using at least one embodiment in accordance with the present invention. The disclosure is further offered to enhance an understanding and appreciation for the inventive principles and advantages thereof, rather than to limit in any manner the invention.

25 It is further understood that the use of relational terms are used solely to distinguish one from another entity or action without necessarily requiring or implying any actual such relationship or order between such entities or actions. Also, the terms use or using in this specification have the broad meaning that includes: viewing, executing, listening, playing, accessing data, accessing information and
30 other similar terms. The reader is specifically drawn to the definition of “device identity” that has the broad meaning of any means, method, technique and the like

associated with the identification of, or identifying, a device or a module on or coupled to a device, and “device identity” includes: an International Mobile Subscriber Identity (IMSI), an International Mobile Equipment Identity (IMEI), internet addresses or any other possible suitable identifier.

5

Much of the inventive functionality and many of the inventive principles are best implemented with or in software programs or instructions and integrated circuits (ICs) such as application specific ICs. It is expected that one of ordinary skill when guided by the concepts and principles disclosed herein will be readily capable of generating such software instructions and programs and ICs with minimal experimentation. Therefore, in the interest of brevity and minimization of any risk of obscuring the principles and concepts according to the present invention, further discussion of such software and ICs will be limited to the essentials with respect to the principles and concepts used by the invention.

15

Turning now to the drawings, wherein like numerals designate like components. Referring to FIG. 1, there is a schematic diagram illustrating an electronics device in the form of a mobile station or mobile telephone 100 comprising a radio frequency communications unit 102 coupled to be in communication with a processor 103. The mobile telephone 100 also has a keypad 106 and a display screen 105 coupled to be in communication with the processor 103. As will be apparent to a person skilled in the art, screen 105 may be a touch screen thereby making the keypad 106 optional.

25

The processor 103 includes an encoder/decoder 111 with an associated code Read Only Memory (ROM) 112 for storing data for encoding and decoding voice or other signals that may be transmitted or received by the mobile telephone 100. The

processor 103 also includes a micro-processor 113 coupled, by a common data and address bus 117, to the encoder/decoder 111, a character Read Only Memory (ROM) 114, a Random Access Memory (RAM) 104, programmable read and write static memory 116, a short range wireless transceiver 180, a plug in memory module and
5 network connection interface 160 and a Removable User Identity Module (RUIM) interface 118. The static programmable memory 116 and a RUIM card 119 operatively coupled to the RUIM interface 118 each can store, amongst other things, Preferred Roaming Lists (PRLs), subscriber authentication data, selected incoming text messages and a Telephone Number Database (TND phonebook) comprising a
10 number field for telephone numbers and a name field for identifiers associated with one of the numbers in the name field. The RUIM card 119 and static memory 116 may also store passwords for allowing accessibility to password protected functions on the mobile telephone 100. As will be apparent to a person skilled in the art the RUIM card 119 is sometimes referred to or is interchangeably referred to as a
15 Subscriber Identity Module (SIM) or Universal Subscriber Identify Module (USIM) and has stored thereon a unique International Mobile Subscriber Identity (IMSI).

The micro-processor 113 has ports for coupling to the keypad 106, screen 105 and an alert 115 that typically contains an alert speaker, vibrator motor and associated
20 drivers. Also, micro-processor 113 has ports for coupling to a microphone 135, a polyphonic speaker 170 and communications speaker 140. The character Read only memory 114 stores code for decoding or encoding text messages that may be received by the communications unit 102. In this embodiment the character Read Only Memory 114, RUIM card 119, and static memory 116 may also store Operating Code
25 (OC) for the micro-processor 113 and code for performing functions associated with the mobile telephone 100. Furthermore, the static memory 116 also stores digital content with corresponding rights object files and a rights expression language described later herein.

The radio frequency communications unit 102 is a combined receiver and transmitter having a common antenna 107. The communications unit 102 has a transceiver 108 coupled to the antenna 107 via a radio frequency amplifier 109. The transceiver 108 is also coupled to a combined modulator/demodulator 110 that couples the communications unit 102 to the processor 103.

FIG. 2 is a block diagram of a system 200 in accordance with an embodiment of the present invention. As shown, system 200 comprises a plurality of electronic devices 201,202,203 typically in form of the mobile station or mobile telephone 100. However, the electronic devices 201,202,203 can be any suitable network connectable devices such as, but not limited to, personal digital assistants, audio players, video players, portable computers and the like. Further, by way of example, one or more of the electronic devices 201,202,203 can be typically equipped to play an MPEG Video Layer 4 file with a standard MPEG video codec. Also, by way of example, one or more of the devices 201,202,203 may be equipped with an application to "play" an MPEG Audio Layer 3 (MP3) file with an application such as a standard MP3 player.

The system 200 also comprises a plurality of content providers 205, 207, 209 and a network 210 allowing communication between electronic devices 201,202,203 (peer-to-peer communications) or communication between any of the content providers 205, 207, 209 and any of the electronic devices 201,202,203. The content providers 205, 207, 209 suitably have databases that provide usable protected digital content to the electronic devices 201,202,203 after executing appropriate DRM protocols governed by usage limitations. For example, content provider 205 may provide protected digital content MP3 files to the electronics device 201 utilizing a DRM protocol as is being developed in MPEG-21 (ISO/IEC TR 21000-1:2001(E) "Part 1: Vision, Technologies and Strategy", available from <http://www.iso.ch/iso/en/ittf/>) while content provider 207 may provide protected digital video content to the

electronic device 202 utilizing a second DRM protocol as described in the Open Mobile Alliance standard as will be apparent to a person skilled in the art. The digital content that may be provided by content providers 205, 207, 209 include, but are not limited to, music, games, video, pictures, books, maps, software, plus any other digital content. Also, the content providers 205, 207, 209 can be communications network providers that provide communications networks and the peer-to-peer communications connections between electronics devices 201,202,203.

In accordance with the exemplary embodiment of the present invention all communication between the electronics devices 201,202,203. and content providers 205-205 takes place over network 202. The network 202 may take various forms such as but not limited to a cellular network, a local-area network, a wide-area network, a hard-wired connection or any other communications network.

FIG. 3 is a conceptual block diagram of what is stored in the static memory 116. As illustrated, the static memory 116 stores programs, files or modules including protected digital content files 310, 314, 318 and respective associated rights files (rights objects) 312, 316, 320 and a DRM agent 330. The static memory 116 also stores programs for system services 340 and programs for applications 305, 307,309. Although this exemplary embodiment illustrates the static memory 116 stores, amongst others, applications 305, 307,309, protected digital content files 310, 314, 318 rights files (rights objects) 312, 316, 320 and the DRM agent 330, it should be noted that any number of storage means could be used for storing one or more of the above. Such storage means can include, but are not limited to, a hard disk storage coupled to interface 160, the Random Access Memory (RAM) 104, and smart card storage device or the RUM card 119 coupled to the RUM interface 118, or a removable memory device such as a Multi-Media Card (MMC) or removable memory coupled to interface 160. Also, as will be apparent to a person skilled in the art, the conceptual block diagram of FIG. 3 is for illustrative purposes only and the programs, files or modules stored in the static memory 116 may be stored by any memory mapping allocation and the mapping may be allocated contiguously or

segmented. It should also be noted that the rights files 312, 316, 320 may be embedded in the protected digital content files 310, 314, 318.

5 In general DRM is enforced and protected, for instance, on the protected digital content file 310 by use of the associated rights file 312. The rights file 312 contains usage permissions and a Content Encryption Key (CEK) for the protected digital content file 310, and the content therein can be rendered or used only by devices having a permitted identifier (ID) possessing rights defined by the corresponding rights file 312. Such rights are given to the device via the identifier
10 (ID) that identifies the device or a module operatively coupled to the device such as an identification code (or number) that on the mobile telephone 100 would typically be an International Mobile Subscriber Identity (IMSI) residing on the RUIM.

15 When protected digital content on the protected digital content file 310 is required to be used by one of applications 305, 307, 309, a device such as the mobile telephone 100 will use the DRM agent 330 to authenticate licenses, parse and enforce rules, and parse, decrypt and consequently access or use the protected digital content in a manner that is governed by access rights provided by the rights file 312. The DRM agent 330 will use the system services 340 to help perform common functions,
20 such as file-system management or decryption of the content in the protected digital content file 310.

25 Consider a model, schema or convention of formatted, compiled or encrypted DRM rights residing in the rights files 312, 316, 320. Such a model, schema or convention suitably comprises, amongst others, permission rights (PR), constraint rights (CR) and security rights (SR). Such models, schemas, or conventions for the DRM rights are generally defined in, for instance, in the Open Mobile Alliance standard DRM Rights Expression Language.

30 Considering the constraints rights (CR), the present invention suitably provides for, amongst others, the following:-

Constraints (CR):

number_of_usages;; expiry_date;
identity;.....; end.

- 5 The number_of_usages constraints rights (CR) specifies the number of times a permission to use an asset may be granted, wherein the permission is defined by the permission rights (PR).

- 10 The expiry_date constraints rights (CR) specifies a time range or time limit for the permission to use an asset may be granted.

The identity constraints rights (CR) specifies an identifier (ID) or identifiers that have the granted permission (PR), defined by the permission rights, to use an asset.

- 15 The present invention makes use of the identity constraints rights (CR), wherein the identity has the following objects:-

- | | | |
|----|----------------------|---|
| | Permitted_Identifier | : <32 bits>; |
| | Match1 | : <10 most significant bits>; |
| | Match2 | : <10 least significant bits>; |
| 20 | Match3 | : <n adjacent bits>; n is an integer between 2 and 31 |
| | Match4 | <n adjacent bits i bits from the least significant bit>; |
| | | Where n and i are integers between 1 and 16 |
| | Match5 | <n adjacent bits i bits from the most significant bit>; |
| | | Where n and i are integers between 1 and 16 |
| 25 | Match6 | : <11 th and 12 th least significant bits>; |
| | Match7 | : <11 th to 15 ^h least significant bits>; |
| | Match8 | : Boolean AND / OR / NOT operators for that can be used on any or all of partial Matches of Match1 to Match7. |

30

From the above identity constraints rights (CR), if a Rights Object Issuer wished to allow use of protected digital content to users, devices, systems or networks

that only have a identifier (ID) with specific 11th to 15th bits (i.e. 460 00) and all other bits were irrelevant, then by selecting only Match7 (all other matches Match1 to 6 and Match8 are un-selected), the Rights Object Issuer will achieve the required protection of allowing use to only identifiers with their 11th to 15th bits matching 460 00. As another example, if the Rights Object Issuer wishes to allow use of protected digital content to users, devices, systems or networks who only have an identifier (ID) with both specific 11th to 15th bits and specific 3rd to 7th bits and all other bits were irrelevant, then by selecting only Match8 (all other matches Match1 to 7 are un-selected), the Rights Object Issuer will achieve the required protection by using Match8 Boolean operators to be coded as: Match7 AND Match3(n=4;i=6). Hence, from the above, it will be apparent that each partial match identifier constraint is allowed to be combined with one or more other partial match identifier constraints by Boolean operators.

Referring to Fig. 4 there is illustrated a flow chart showing a method 400 of operation of the communication system 200. The method 400 is initiated at a start block 410, by a suitable connection of one of devices 201, 202, 203 to one of the content providers 205, 207, 209, by the network 210. The method 400, at a block 420, performs providing protected digital content and an associated rights object at a block 420. The providing is performed over the network and can be Multimedia Messaging or downloading from a website or any other form of providing. By way of example, if the network 210 is a cellular network then the providing can be performed by the Content provider 205 (who is essentially a rights object issuer) sending the protected digital content and an associated rights object in one or more Multimedia Messages to the mobile telephone 100.

At a block 430, there is performed receiving and storing the protected digital content and an associated rights object in the static memory 116. The receiving is via the radio frequency communications unit 102 and, for example, the protected digital content is stored in the protected digital content file 310 and the rights object is stored in the rights file 312. The protected digital content file 310 and the rights object stored in the rights file 312 can be received separately in one transmission or they can

be received in two separate transmissions. Also, the rights object may be embedded in the protected digital content file 310.

As will be apparent to a person skilled in the art, when the providing is performed the content provider 205 obtains an identifier (ID) from the device this identifier (ID) is the International Mobile Subscriber Identity (IMSI) stored in the RUIM 119 or SIM or USIM, however other forms of identifier (ID) can be used including an International Mobile Equipment Identity (IMEI), internet addresses or any other possible suitable identifier depending typically on the type of system 200 and requirements of the content provider 205. In this exemplary embodiment, this identifier (ID) is a permitted identifier (PID) that is stored in the 32 bit Permitted_Identifier object/field in the identity constraints rights (CR) that is included in the provided rights object. It should be noted that not all 32 bits may be used in the Permitted_Identifier object/field and in one embodiment permitted identifier (PID) stored in the Permitted_Identifier object/field may be a telephone number corresponding to an International Mobile Subscriber Identity (IMSI) or any other identifier (ID) such as an IMEI, internet addresses or any other possible suitable identifier could be used. Also provided in the rights object is at least one partial match identifier constraint (Match1 to Match8) that is allowed by the identity constraints rights (CR). The partial match identifier constraint may be adjacent digits (bits) in a telephone number corresponding to an International Mobile Subscriber Identity. The adjacent bits may be adjacent least significant bits or an adjacent most significant bits. The adjacent bits may identify a networks provider, or may identify a country, region, state or city. The least one partial match identifier constraint may suitably include matching: a 10 most significant bits of the identifier; 10 least significant bits of the identifier; n adjacent bits of the identifier; n adjacent bits i bits from the least significant bit of the identifier; n adjacent bits i bits from the most significant bit of the identifier 11th and 12th least significant bits of the identifier; or 11th to 15^h least significant bits of the identifier, wherein n and i are integers.

30

After block, 430, the method 400 may terminate or effect further providing and receiving of more protected digital content and an associated rights object may be

performed. However, at some point the mobile telephone 100 may be sent a user command, input at the keypad 106, requesting usage of the protected digital content. As illustrated, the requesting usage is performed immediately after block 430 completes the receiving and storing.

5

The requesting usage of the protected digital content is performed at a block 440, typically in response to the user command input at the keypad 105 (or automatically upon the receiving and storing of block 430. The requesting usage of the protected digital content is for the content to be used by an application supported
10 by the mobile telephone 100 that has a device identity, for instance, the identifier (ID) obtained from the International Mobile Subscriber Identity (IMSI). If for example the protected digital content in file 310 is an encrypted MPEG Video Layer 4 file then, at a block 450, the method 400 performs reading the rights object in rights file 312 associated with and governing allowed use of the protected digital content in file 310.
15 Also one of applications 305,307, 309 capable of running MPEG Video Layer 4 files is selected to be used by the mobile telephone 100.

Next, at a block 460, the method 400 performs determining from the rights object in file 312 the DRM rights including: the permitted identifier (PID) or
20 permitted identifiers from the Permitted_Identifier object/field; and, if included in the identity constraints rights (CR), at least one partial match identifier constraint of Match1 to Match8 that has been set/selected.

A test is then conducted, at a match test block 470, to check if the permitted
25 identifier (PID) in the rights object file 312 either: exactly matches the device identity obtained from the identifier (ID); or partially matches the device identity obtained from the identifier (ID) as stipulated by the at least one partial match identifier constraint defined by the allowed set/selected matches (Match1 to Match8). If there is no match or partial match at block 470 then the method, at block 480,
30 provides for disallowing use of the protected digital content stored in file 310. Alternatively, if there is a match or partial match, based on the above matching criterion, then the method, at block 490 provides for allowing the use, governed by

the rights object in file 312, of the protected digital content in file 310 by the mobile telephone 100 only when the device identity obtained from the identifier (ID) exactly matches the permitted identifier (PID) or partially matches the permitted identifier (PID) as stipulated by the at least one partial match identifier constraint defined by the allowed matches (Match1 to Match8). Hence, the DRM agent 330, assisted by the system services decrypts, using the Content Encryption Key (CEK) in the rights object and plays the protected digital content in file 310 (an encrypted MPEG Video Layer 4 file) using application 305 (an MPEG player) on the screen 105 complemented by the polyphonic speaker 170. The method 400 then terminates, after block 480 or 490, at an end block 495.

Advantageously, if the content provider, or copyright owner or licensee, wishes to provide or allow use of their protected digital content to specific groups or regions then a suitable one or more of the at least one partial match identifier constraints defined by the allowed matches (Match1 to Match8) of the identity constraints rights (CR) can be set in the rights object. Hence, the content provider, or copyright owner or licensee can selectively allow large groups, specific subscription tiers, and regions to use and distribute via their radio communications unit 102 over a network, by hard wired connections or plug in devices using the interface 160, or by the short range transceiver 180 or by any other means. For example, if the device identity obtained from the identifier (ID) corresponds to the telephone number 65 123456789 then if Match3 is selected to be included in the rights object and n is set to 2 then any telephone number with 2 adjacent bits matching any of the two adjacent bits of 65 12345678 will be able to use the protected digital content. However, to provide a tighter limitation on which groups can use the protected digital content then match4 can be used such that n is set to 2 and i is set to 8, hence only telephone numbers with 65 with their 9th and 10th digits (bits) will be able to use the protected digital content. Since 65 in the 9th and 10th digits (bits) of a telephone number are the country code for Singapore then the group of users are those with mobile telephones having an identifier (telephone number) with an IMSI number for Singapore.

Another example targets to the different operators scenario. One of the IMSI number segments assignment to one mobile operator in China is the segment 460 00 XXXXX XXXXX, this means one International Mobile Subscriber Identity (IMSI) with the first 5 Most Significant Bits equals 460 00 belongs to this mobile operator.

5 For another operator in China, the International Mobile Subscriber Identity (IMSI) segment starts with 460 01. Accordingly, if the partial match in the rights object was defined for the 5 bits from the first most significant bit, and the User_Identifier in the Rights Object was written by a Rights Object Issuer as 460 00 XXXXX XXXXX, the subscriber of any other mobile operator can not get the permission to access the

10 protected digital content.

Only a few examples of the advantages of the present invention have been provided with specific reference to IMSI numbers providing the device identity, however, it will be apparent to a person skilled in the art that the device identity and

15 permitted_Identifier (PID) may be any other possible allowable identifier including, but not limited to, the identifiers specifically referred to in this specification.

The above detailed description provides an exemplary embodiment only, and is not intended to limit the scope, applicability, or configuration of the present

20 invention. Rather, the detailed description of the exemplary embodiment provides those skilled in the art with an enabling description for implementing the exemplary embodiment of the invention. It should be understood that various changes can be made in the function and arrangement of elements and steps without departing from the spirit and scope of the invention as set forth in the appended claims.

25

Claims

1. A method for DRM of protected digital content, the method including:
Requesting usage to protected digital content to be used by an application
5 supported by an electronics device having a device identity associated therewith;
reading a rights object associated with and governing allowed use of the
protected digital content;
Determining from the rights object an identifier and at least one partial match
identifier constraint; and
10 Allowing the use, governed by the rights object, of the protected digital
content by the device only when the device identity exactly matches the identifier or
partially matches the identifier as stipulated by the at least one partial match identifier
constraint.
- 15 2. A method for DRM of protected digital content, as claimed in claim1, wherein
the identifier is a user identifier identifying a user of the device.
3. A method for DRM of protected digital content, as claimed in claim2, wherein
the identifier is a user identifier of an RUIM or SIM or USIM.
20
4. A method for DRM of protected digital content, as claimed in claim1, wherein
the identifier is an International Mobile Subscriber Identity or an International Mobile
Equipment Identity number.
- 25 5. A method for DRM of protected digital content, as claimed in claim 4,
wherein the least one partial match identifier constraint are adjacent bits in the
International Mobile Subscriber Identity.
- 30 6. A method for DRM of protected digital content, as claimed in claim 5,
wherein the adjacent bits are adjacent least significant bits or an adjacent most
significant bits.

7. A method for DRM of protected digital content, as claimed in claim 6, wherein the adjacent bits identifies a networks provider, or may identify a country, region, state or city.

5

8. A method for DRM of protected digital content, as claimed in claim 1, wherein the least one partial match identifier constraint includes matching from one or more of the following: a 10 most significant bits of the identifier; 10 least significant bits of the identifier; n adjacent bits of the identifier; n adjacent bits i bits from the least significant bit of the identifier; n adjacent bits i bits from the most significant bit of the identifier 11th and 12th least significant bits of the identifier; or 11th to 15^h least significant bits of the identifier, wherein n and i are integers.

9. A method for DRM of protected digital content, as claimed in claim 8, wherein each partial match identifier constraint is allowed to be a combined with one or more other partial match identifier constraints by Boolean operators.

10. A device comprising:
a memory storing both a protected digital content file and associated object rights, the object rights having an identifier and at least one partial match identifier constraint;
a processor operatively coupled to the memory,
at least one user interface and a keypad operatively coupled to the processor, wherein in response to a user command provided at the keypad the device determines from the rights object an identifier and at least one partial match identifier constraint, and thereafter allows the use by the user interface, governed by the rights object, of the protected digital content by the device only when the device identity device that identifies the device exactly matches the identifier or partially matches the identifier as stipulated by the at least one partial match identifier constraint.

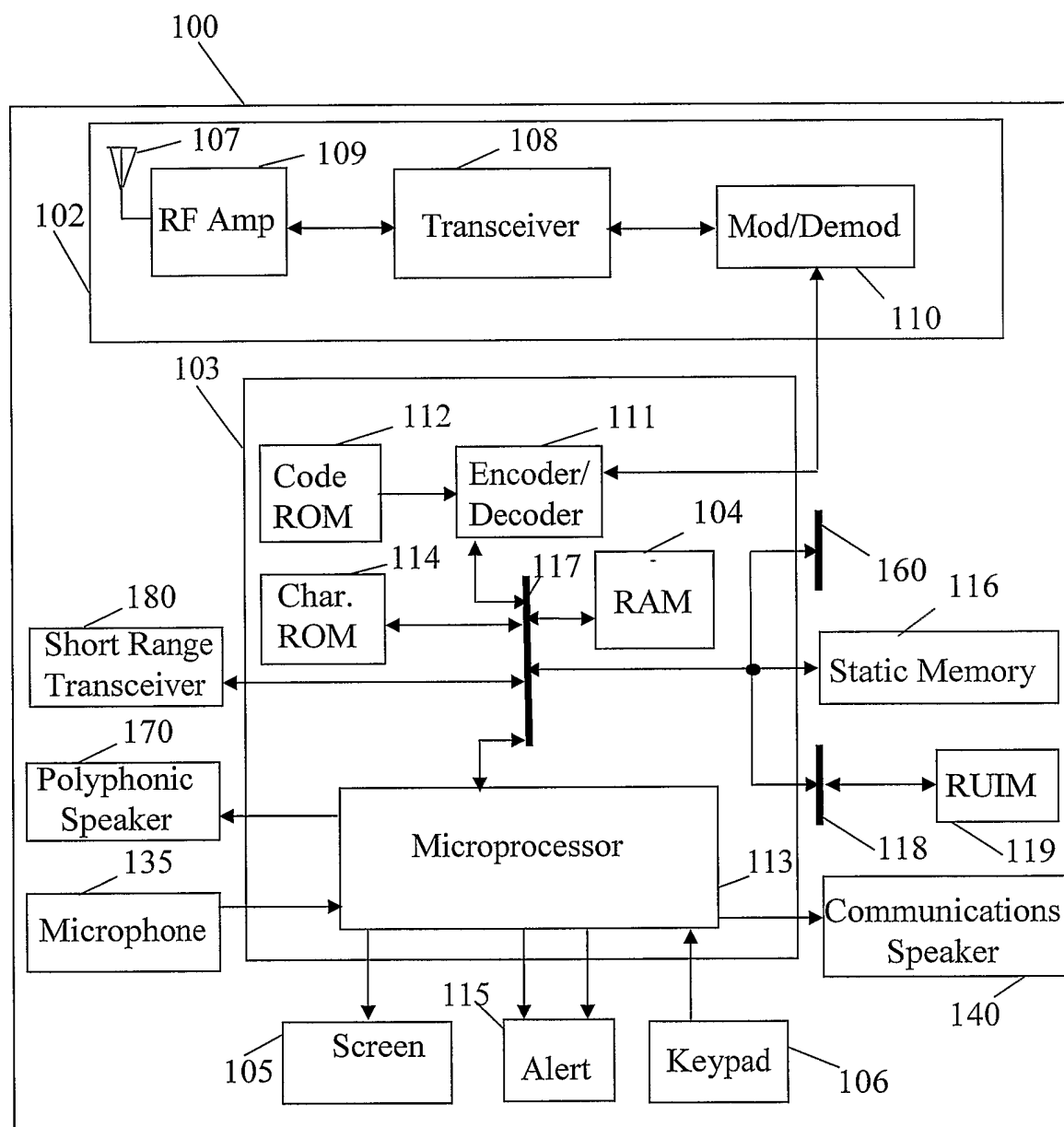
30

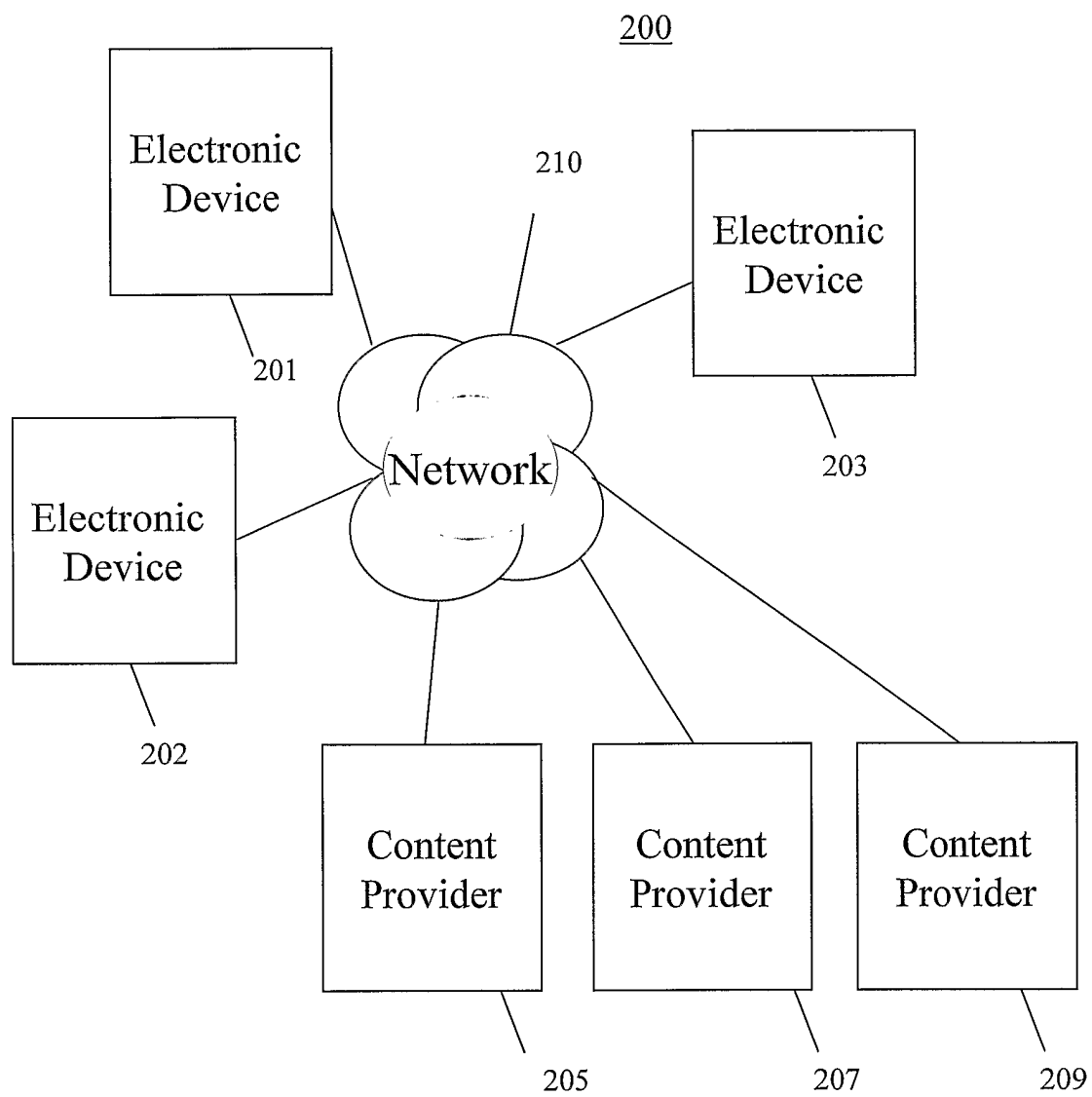
11. A device, as claimed in claim 10, wherein the identifier is a user identifier identifying a user of the device.

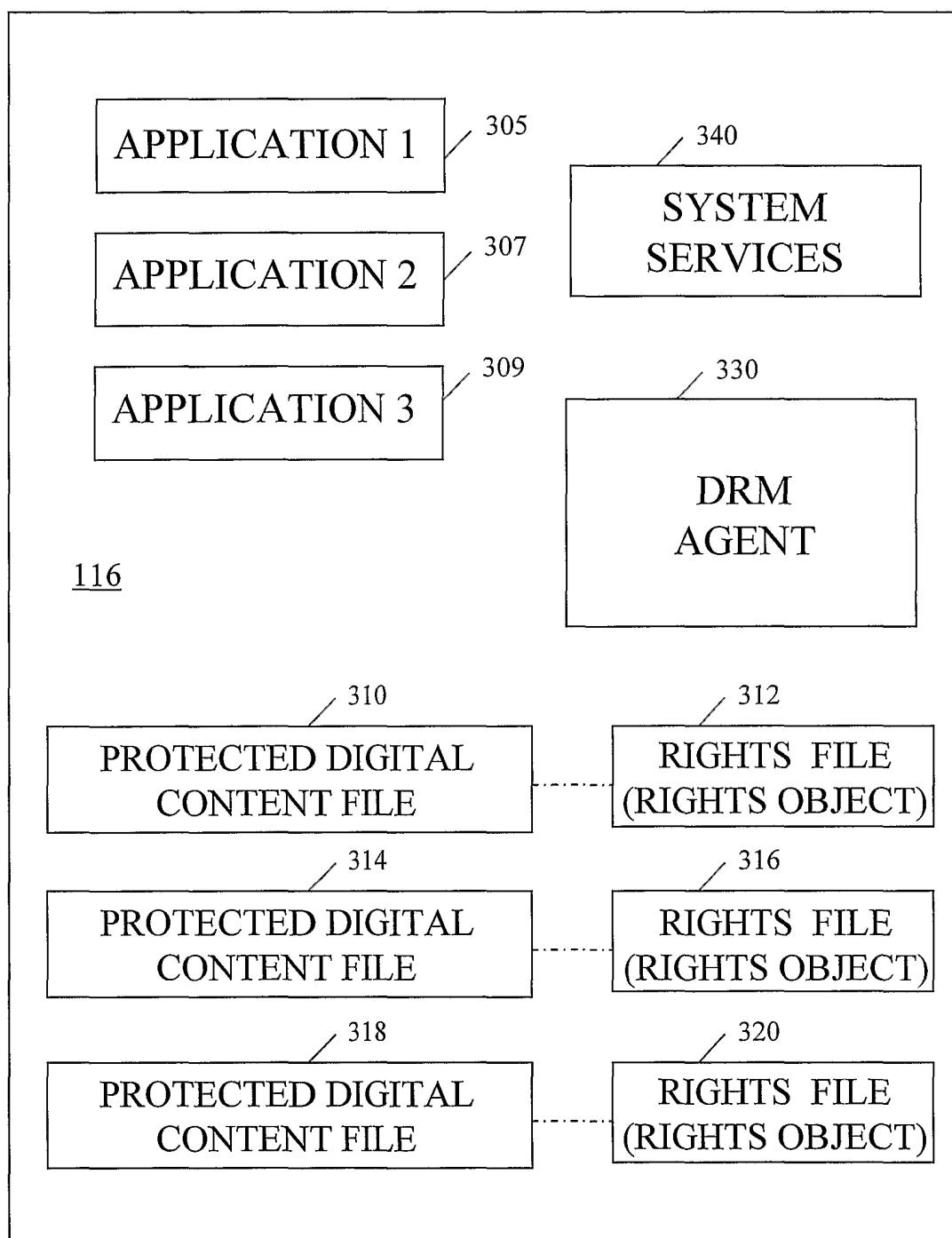
12. A device, as claimed in claim 11, wherein the identifier is a user identifier of an RUIM or SIM or USIM.
- 5 13. A device, as claimed in claim 10, wherein the identifier is an International Mobile Subscriber Identity or an International Mobile Equipment Identity number.
14. A method for providing protected digital content, the method including:
Obtaining a device identity from a device to which the protected digital
10 content is to be provided; and
Providing the protected digital content and an associated rights object, wherein the rights object contains an identifier obtained from the device identity and at least one partial match identifier constraint.
- 15 15 A method for providing protected digital content, as claimed in claim 14, wherein the identifier is a user identifier identifying a user of the device.
16. A method for providing protected digital content, as claimed in claim 15, wherein the identifier is a user identifier of an RUIM or SIM or USIM.
- 20 17. A method for providing protected digital content, as claimed in claim 14, wherein the identifier is an International Mobile Subscriber Identity or an International Mobile Equipment Identity number.
- 25 18. A method for providing protected digital content, as claimed in claim 16, wherein the least one partial match identifier constraint is adjacent bits in a telephone number corresponding to an International Mobile Subscriber Identity.
- 30 19. A method for providing protected digital content, as claimed in claim 14, wherein the least one partial match identifier constraint may suitably include matching from one or more of the following: a 10 most significant bits of the identifier; 10 least significant bits of the identifier; n adjacent bits of the identifier; n adjacent bits i bits

from the least significant bit of the identifier; n adjacent bits i bits from the most significant bit of the identifier 11th and 12th least significant bits of the identifier; or 11th to 15^h least significant bits of the identifier, wherein n and i are integers.

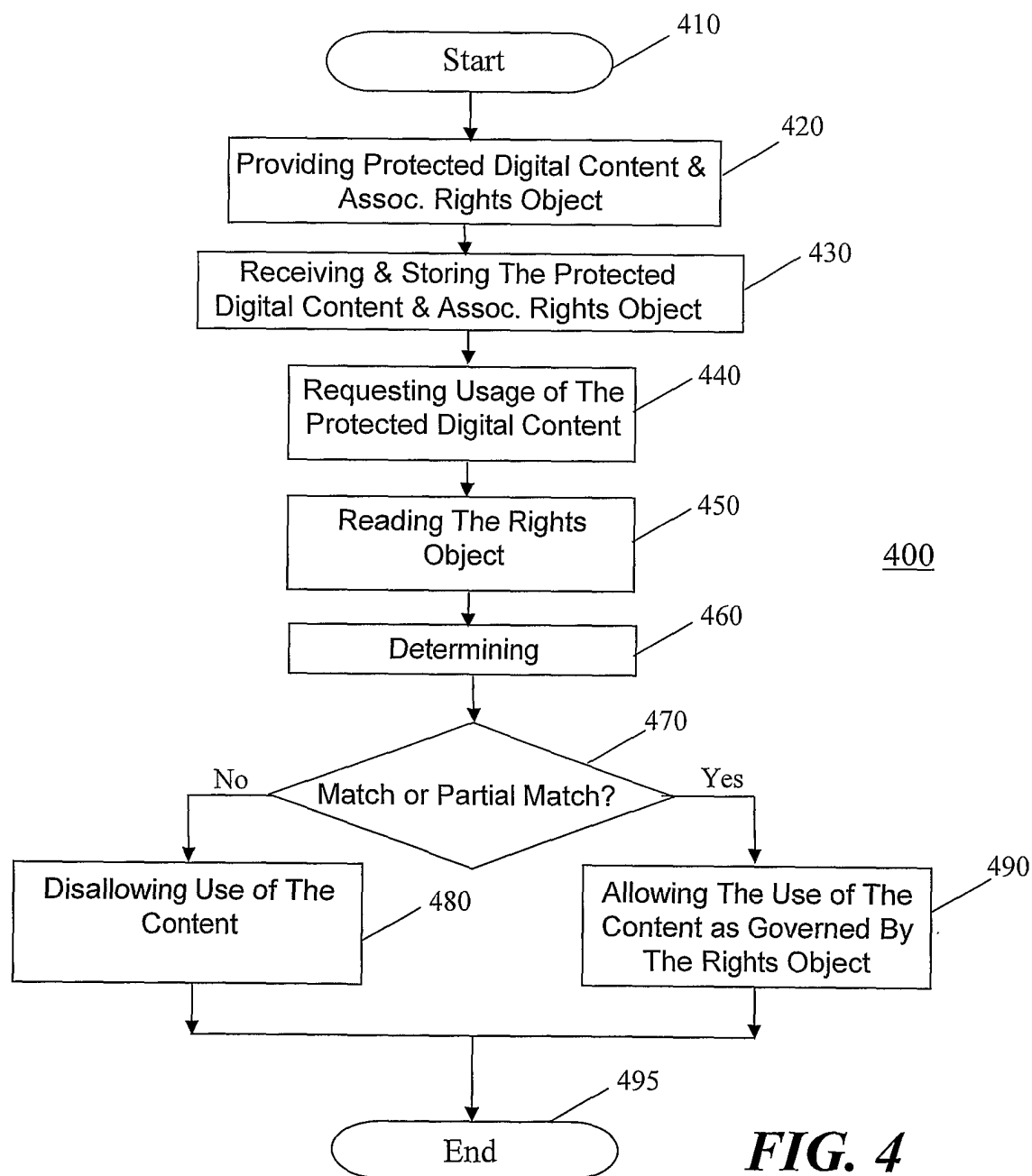
- 5 20. A method for providing protected digital content, as claimed in claim 14, wherein each partial match identifier constraint is allowed to be a combined with one or more other partial match identifier constraints by Boolean operators.

1/4*FIG. 1*

2/ 4**FIG. 2**

3/4**FIG. 3**

4/4

**FIG. 4**