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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 June 2005 (23.06.2005)

PCT

(10) International Publication Number
WO 2005/057346 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number:
PCT/US2004/040486

(22) International Filing Date: 2 December 2004 (02.12.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/727,332 2 December 2003 (02.12.2003) US

(71) Applicant *(for all designated States except US)*: **BROADON COMMUNICATIONS CORP.** [US/US]; 3400 Hillview Avenue, Building 5, Palo Alto, CA 94304 (US).

(72) Inventors: **YEN, Wei**; 27886 Via Ventana, Los Altos Hills, CA 94022 (US). **PRINCEN, John**; 10439 Plum Tree Lane, Cupertino, CA 95014 (US). **LO, Raymond**; 1429 Meadow Lane, Mountain View, CA 94040 (US). **SRINIVASAN, Pramila**; 1853 Channing Avenue, Palo Alto, CA 94303 (US).

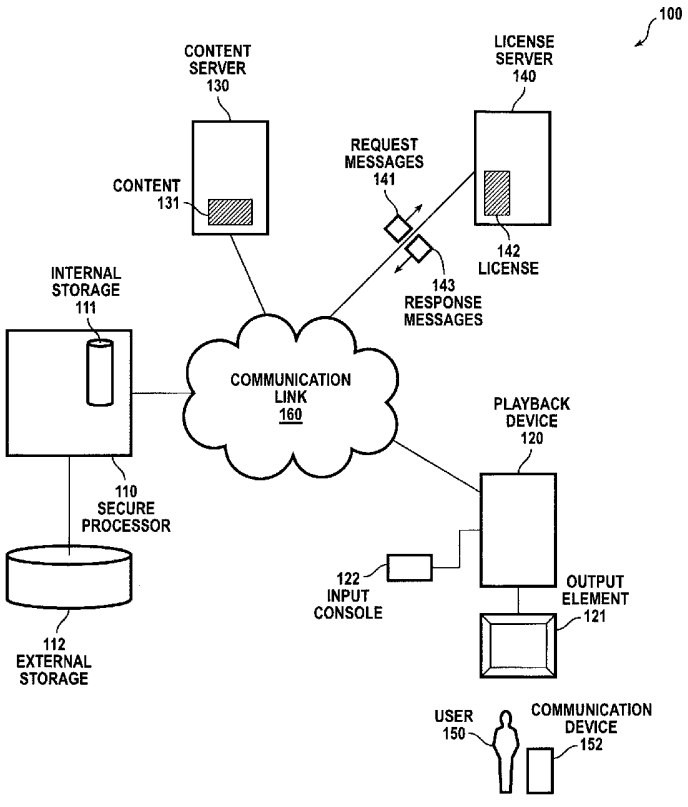
(74) Agent: **COLEMAN, Brian, R.**; Perkins Coie LLP, P.O. Box 2168, Menlo Park, CA 94026-2168 (US).

(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, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, 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,

[Continued on next page]

(54) Title: DELIVERY OF LICENSE INFORMATION USING A SHORT MESSAGING SYSTEM PROTOCOL IN A CLOSED CONTENT DISTRIBUTION SYSTEM



(57) Abstract: Delivery of licenses (142) in a closed distribution system including a playback device (120) and secure processor (110). The secure processor (110) allows only use of authorized content (131), and the playback device (120) is authorized to execute content (131). A user (150) requests a license (142) to selected content (131) using a communication link, without the playback device (120), outside the closed content system to a license server (140). The user (150) requests licenses (142) using SMS, sending small amounts of information, possibly including proofs of purchase. The server (140) responds using SMS, providing the user (150) with a code representing information interpretable as a license, such as an encrypted content key or a shared secret known to the user (150). The user (150), using a keypad or other device (122), inputs that code to the playback device (120), which determines if it authorizes use of the content (131). The playback device (120) authenticates the license (142), determining whether that license (142) authorizes the use (150) for the content (131), and enforces the licensed rights.

WO 2005/057346 A2

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, 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).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations 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, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for all designations*

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.

DELIVERY OF LICENSE INFORMATION USING A SHORT MESSAGING SYSTEM PROTOCOL IN A CLOSED CONTENT DISTRIBUTION SYSTEM

Background of the Invention

1. *Field of the Invention*

The invention relates to out-of-band delivery of license information, such as for example using an SMS (short messaging system) protocol, with the effect of delivering that license information to a destination in a closed content distribution system, using, at least in part, a channel other than that used for content distribution itself.

2. *Related Art*

Closed content distribution systems include end-to-end systems, including publishing servers, content distribution servers and playback devices, where the content that is playable on playback devices can be completely controlled through appropriate security techniques, and those security techniques make it relatively difficult for any unauthorized third party to distribute content that would be playable on the playback devices.

One example of a closed content distribution system includes a playback device, such as a game station, such as for example found in an arcade, a user's home, or a similar type of location, using which content can be executed or presented interactively with one or more game players. Content can be distributed to such a playback device using a download connection to a distribution network, or using transport of physical media (such as for example CD-ROMs or DVDs) including the content, possibly encrypted using a symmetric key, or possibly encrypted using an key pair such as in a public key cryptosystem. For one example, not intended to be limiting in any way, the playback device might operate alone or in conjunction or cooperation with other devices, such as for example a display monitor or an input controller.

One concern with closed content distribution systems is how information is distributed from authorized sources to those playback devices, how those playback devices

determine if license rights associated with the user permit that user to execute or present that content, and how those playback devices enforce those license rights while executing or presenting that content. For one example, not intended to be limiting in any way, the closed content distribution system can include reception by the playback device of (1) content to be executed or presented, and of (2) *licenses* indicating scope of rights by users to execute or present that content.

One problem is that requirements of channels for distribution of content and licenses can differ significantly, including the amount of information for distribution, the frequency or timing of those distributions, and the degree of time latency tolerable for those distributions. It might be common to distribute several gigabytes of information for content, using one or more DVDs once per week, and to accept a time latency of several days for that distribution. In contrast, it might be common to distribute at most several kilobytes of information for licenses, but it might be advantageous to receive that license information within minutes of a request, such as for example in response to the user presenting proof of payment for the license.

For one example, not intended to be limiting in any way, it might be advantageous to allocate a function of delivering content to a content server, and separately to allocate a function of delivering licenses to a license server. One problem is that contact with such a license server involves relatively more frequent requests for relatively smaller amounts of information, and should provide for relatively quick response and relatively little time latency. In contrast, contact with such a content server involves relatively less frequent requests for larger amounts of information, and can tolerate relatively slower response and relatively larger time latency. In one embodiment, the license enables the content to be determined to be executable, valid, or both, with the effect that the content might be received at the player device any time in advance of the license.

If content is to be delivered to the playback device using physical media, distribution does not need to involve any coupling to a communication network or other form of electronic distribution. However, if licenses are to be delivered to the playback device, coupling to a communication network or other form of electronic distribution can involve significant expense, particularly when the playback device is itself relatively

inexpensive. Also, this would involve network connectivity or other connectivity being available at the consumer end (that is, the playback device itself), when communicating with the license server. Accordingly, it would be advantageous to provide a technique for delivering licenses relatively quickly and with relatively little time latency, without involving the expense of coupling the playback device to a communication network or other form of electronic distribution.

Accordingly, it would be advantageous to provide a technique involving delivery of license information or a shorter code from which license information might be derived or verified, not subject to drawbacks of known systems, such as for example in a closed distribution system.

Summary of the Invention

The invention provides a method and system capable of delivery of license information, such as for example in a closed distribution system. In one embodiment, a closed distribution system includes a playback device including a computing device capable of general purpose processing, and capable of enforcing mandatory execution of selected security software, such as for example a secure processor. The playback device is capable of receiving content to be executed or presented, such as for example embedded on physical media delivered to a location at or near the playback device. Operation of the secure processor assures that only authorized content is executed or presented by the playback device, and any appropriate licensing or rights information is interpreted and enforced by the playback device. In one embodiment, the secure processor has access to external memory on which that secure processor can maintain rewritable information, such as for example game state information, license information, and user information, authenticated or hidden using a cryptographically-secure technique, such as for example digital encryption or digital signature.

For one example, not intended to be limiting in any way, the playback device might be coupled to a LAN (local area network) or a secured enterprise network, with the effect that content delivered to devices coupled to one of those networks can be available to

the playback device. This includes the effect that the playback device would be able to include additional communication links to supplemental input controllers, with the effect that the method and system can support multiplayer games and games with multiple input controllers, and with the effects that games can include contests among multiple players for "high score" and the like, and can also include associations of players, such as for example player teams.

In one embodiment, a user (such as a game-player) associated with a playback device makes a connection to a license server, to request a license to selected content. The connection includes a communication link outside the closed content system, and provides the user with a technique for communicating with the license server, without involving the playback device in that connection. For one example, not intended to be limiting in any way, the user might request a license using SMS (short messaging system) or another technique with the effect of sending a relatively small amount of information to request a license for specific content (whether application program, media content, or otherwise). The license server receives the request, determines if a license should be issued, and responds to the request. For one example, not intended to be limiting in any way, the license server might respond to the request using SMS, with the effect of providing the user with an alphanumeric or numeric code. This has the effect of allowing the user to input that alphanumeric or numeric code to the playback device, which can determine if that alphanumeric or numeric code authorizes the user for the selected content.

In one embodiment, the alphanumeric or numeric code might represent information included in a license message. For one example, not intended to be limiting in any way, the alphanumeric or numeric code might include a hexadecimal (or other radix) representation of a license message. The playback device might receive that alphanumeric or numeric code from the user using a keypad or other input device.

In one embodiment, the playback device, using its secure processor, can authenticate the license message, with the effect of determining whether the user is authorized to execute or present the selected content. For one example, not intended to be limiting in any way, the license message might be encoded using a digital signature or a secure hash, with the effect that the playback device (or the secure processor) can determine

if that license message is authentic. If that license message is in fact authentic, the playback device (or the secure processor) can determine if that license message grants the user sufficient rights to execute or present the selected content, and can control whether that selected content is executed or presented.

For a first example, not intended to be limiting in any way, the alphanumeric or numeric code might include a representation of a content decryption key, using which the playback device might be able to decrypt content and access that content for execution or presentation. In one embodiment, content encryption and decryption includes a public-key cryptosystem, with the effect that the content decryption key would include a decryption key privately associated with the content, encrypted by an encryption key publicly associated with the specific playback device. This would have the effect that the alphanumeric or numeric code would only allow the playback device to execute or present the content if the selected content and the specific playback device were both associated with the information received from the license server.

For a second example, not intended to be limiting in any way, an activation code might include an identity of the player and an identity of the content itself, either signed by the license server, or encrypted by a common key (such as for example a Diffie-Hellman shared secret) that can be computed by both the license server and the specific player. The mandatory security software would, in such cases, enforce the computation of the secret key (using its private key and server public key) and decryption of the identities. In alternative embodiments, the mandatory security software may enforce the verification of a signature by the license server. In such cases, the mandatory security software would force the comparison of the player identity with its own tamper-proof identity and the identity of the content that the activation code is meant for. In such cases, the mandatory security software would separately authenticate the content identity with respect to the content data hash or signature, using a trusted server (such as for example a trusted content publisher) signature over those quantities.

In one embodiment, communication between the license server and the user involves a commercial transaction. For one example, not intended to be limiting in any way, the license server would receive information from the user sufficient to allow the license

server to effect a purchase transaction by the user (such as for example, a credit card or debit card number the user is authorized to charge, an account or a subscription the user is authorized to use, and the like). In such embodiments, the license server would issue the alphanumeric or numeric code in response to the user having sufficient authorization to use the playback device; that sufficient authorization would include proof that the user had (either in the past or just then) purchased the right to use the content with that playback device.

After reading this application, those skilled in the art would recognize that the techniques described herein provide an enabling technology, with the effect that heretofore advantageous features can be provided that heretofore were substantially infeasible.

Brief Description of the Figures

Figure 1 shows a block diagram of a system including a closed distribution system and a separate connection capable of delivery of license information.

Figure 2 shows a process flow diagram of a method of using a system including a closed distribution system and a separate connection capable of delivery of license information.

Related Disclosure

This application is related to the following document:

- International patent application number PCT/US2004/003413, "Secure and Backward-Compatible Processor and Secure Software Execution Thereon," in the name of BroadOn Communications Corporation, filed on 6 February 2004 and published on 26 August 2004 under publication number WO 2004/072787 A2.

This document is sometimes referred to herein as the "related disclosure."

Inventions described herein can be used in combination or conjunction with technology described in related disclosure.

Detailed Description of the Preferred Embodiment

Preferred embodiments of the invention are described herein, including preferred device coupling, device functionality, and process steps. After reading this application, those skilled in the art would realize that embodiments of the invention might be implemented using a variety of other techniques not specifically described herein, without undue experimentation or further invention, and that such other techniques would be within the scope of the invention.

Lexicon

The following terms refer or relate to aspects of the invention or its embodiments. The general meaning of each of these terms is intended to be illustrative and in no way limiting.

- The phrase "closed distribution system" generally describes a system in which content can be delivered from an authorized source, and in which recipients of that content can assure that the specific content is authorized to be executed or presented in the closed distribution system. The concept of a closed distribution system is broad, and includes any system in which distribution, execution, or presentation of content can be restricted to specific authorized content. In one embodiment, the closed distribution system can be used in combination or conjunction with business techniques in which content can be licensed or paid for by those users who wish to execute or present that content.

- The term "content" or the phrase "content element" generally describe an application program (such as for example a game program) or a set of media content (such as for example an animation clip or a video clip) to be executed or interpreted (for code or instructions) or to be displayed or presented (for media content). As described

below, the content might include application software, audio/video presentations, databases, games, multimedia content, reasonable combinations or generations thereof, and the like. The concept of content is broad, and might include application programs, games, audio or video, and the like. In one embodiment, each content item is associated with a unique identity, with the effect that licenses can refer to that specific content item.

- The phrase "secure processor" generally describes any device that can use information from a rewritable storage element, and can operate as a relatively secure computing device performing the functions of a controller for a game system or similar system. As described below, the secure processor is relatively secure against tampering, and includes at least a UID (unique identifier) or a known encryption key (such as for example a key private key of a private-public key pair in a public-key cryptosystem), with the effect that other elements of the system are capable of communicating privately and securely with the secure processor. The concept of a secure processor is broad, and includes any general purpose or special purpose computing device for which there is at least some secure memory, secured against inspection or intrusion from outside the secure processor, and for which there is at least some executive control capable of preventing application software from disclosing the contents of that secure memory. In one embodiment, the secure processor has at least some built-in security software that cannot readily be circumvented or other techniques to securely bootstrap the loading of such security software from insecure devices, such as for example external mass storage.

- The phrase "playback device" generally describes any device that can execute or present selected content, such as for example in conjunction with, in cooperation with, or under control of a relatively secure computing device, such as possibly a secure processor as described above. As described below, this has the effect that the playback device is relatively secure against tampering, with the effect that only authorized users can execute or present content using the playback device. The concept of a playback device is broad, and includes any general purpose or special purpose computing device capable of executing instructions or presenting human-readable media (such as for example audio or visual media). In one embodiment, the

playback device has at least some built-in security software that cannot readily be circumvented. In one embodiment, (1) each playback device is associated with a unique identity, with the effect that licenses can refer to that specific playback device, and (2) each playback device is associated with a public/private key pair in a public key cryptosystem, with the effect that other devices can communicate securely with that playback device.

- The term "license" generally describes information sufficient for the secure player to verify the authenticity of the content and to use the content, and to verify that the specific user has rights to execute or present the content at the specific playback device. In one embodiment, each license includes a data structure associated with one or more content elements, and including, in one embodiment, (1) a key for that content, such as for example encrypted by an encryption key publicly associated with the user or including a shared secret known to the user, with the effect that the secure processor can access the content if it has access to the license, (2) a digital signature or secure hash value, with the effect that the license cannot be easily altered and remain effective, and (3) a digital signature or secure hash value associated with the content itself, with the effect that the license can be verified by the playback device to be associated with the specific content. As described below, the license also includes a description of those rights the licensee has with regard to the content. In one embodiment, licenses are individually tailored to each authorized recipient or user, although in the context of the invention there is no such particular requirement.

- The phrase "activation code" describes a part of a whole license, considered necessary and sufficient to permit execution of selected specific content by the specific player device. An activation code might be an entire license, a part thereof, or a transformation thereof (such as a transformation suitable for human reading or data entry).

- The phrase "license server" generally describes, in the distribution system, any device capable of delivering licenses or activation codes granting rights to content. In one embodiment the license server includes an online transaction server capable of requesting an identity of the device requesting the license and capable of creating, in

response, a cryptographically signed data structure containing information specifying a content item identity, a playback device identity and a set of rights to that content.

- The term "rights" and the phrases "content rights" or "rights to the content" generally describe what actions the secure processor and the playback device re allowed to take with regard to the content. For some examples, not intended to be limiting in any way, the rights might include a number of times the secure processor or the playback device are allowed to execute the content, an amount of total running time the secure processor or the playback device are allowed to execute the content, an amount of wall-clock time the secure processor or the playback device are allowed to execute the content, what resources (such as for example what hardware or what software) the secure processor or the playback device can utilize during execution or presentation of the content, and the like. As described below, the secure processor prevents any use of the content outside those specified by the content rights.

- The phrases "content server" or "content distribution server" generally describe, in the distribution system, any device capable of delivering content (either directly or indirectly), to a secure player or secure processor, using any form of transport technique. As described below, the content distribution server needs only a single copy of each content element, and might deliver multiple individualized copies of that content element in response to distinct users or in response to distinct requests. The concept of a content server is broad, and includes not only a server having content stored thereon, but also devices by which content might be dynamically created, such as a television camera, video camera, webcam, any reasonable generalization thereof, and the like. The content server may include a secure device capable of generating a secure hash and securely signing any information distributed from the server.

- The phrase "input console" generally describes any device capable of delivering control inputs, either directly or indirectly, from a user to a playback device or a controller thereof. The concept of an input console is broad, and includes any manner of user input device, possibility including a keyboard or keypad, joystick or mouse or other pointing device, or other control buttons, whether pre-selected or

dynamically presented using a flat-panel controller, and the like. For example, the input console might include a direct wire connection, a direct RF or IR connection, or an indirect (switched) connection.

- The term "rewritable storage element" generally describes any device capable of maintaining information for use by a secure processor or playback device, and capable of being rewritten with new information. As described below, a rewritable storage element might include a flash memory. The concept of a rewritable storage element is broad, and includes any manner of storage device capable of being read and written, whether random access or not, and whether the read or write operations are relatively rapid or not. For some examples, not intended to be limiting in any way, the rewritable storage element might include an SRAM, flash memory, bubble memory, or disk drive (magnetic or optical or both).

The scope of the invention is not limited to any of these definitions, or to specific examples mentioned therein, but is intended to include the most general concepts embodied by these and other terms.

System Elements

Figure 1 shows a block diagram of a system including a closed distribution system and a separate connection capable of delivery of license information.

A system 100 includes a secure processor 110, a playback device 120, a content server 130, a license server 140, and a communication link 160 between the license server 140 and a user 150.

As further described in the related disclosure, the secure processor 110 includes a secure state and its monitored state, with an application program (such as a game program) running in the monitored state. In one embodiment, the application program is responsive to a set of content 131, suitable for execution or presentation. The secure processor 110 might perform the content 131 in the monitored state, where that content 131

is suitable for execution, or might control the playback device 120 to present the content 131, where that content 131 is suitable for presentation.

In one embodiment, the secure processor 110 includes at least some internal storage 111, suitable for maintaining data secure against discovery or tampering, and is associated with a unique identifier and with a public/private key pair in a public key cryptosystem. The secure processor 110 also includes at least some external storage 112, such as for example flash memory or one or more disk drives, on which the secure processor 110 might maintain additional information (such as information not readily capable of being maintained in the internal storage 111). In one embodiment, the additional information maintained on the external storage 112 can be protected against discovery by digital encryption and can be protected against tampering using a digital signature or a secure hash code.

The playback device 120 includes an output element 121 capable of presenting the content 131, and includes at least one input console 122 capable of receiving commands, control inputs, or other inputs from one or more users 150. In one embodiment, the playback device 120 is capable of receiving control inputs from the input console 122, such as for example a set of license information received from the license server 140.

In one embodiment, the secure processor 110 and the playback device 120 are effectively coupled, with the effect that the secure processor 110 can execute the content 131, or can control the playback device 120 to present the content 131. For a first example, not intended to be limiting in any way, the playback device 120 might include a computer game station operating under control of an embedded secure processor 110 (and possibly other processors). For a second example, not intended to be limiting in any way, the playback device 120 might include audio, video, or audio-video presentation hardware, capable of presenting sound and pictures to the user 150 in response to control of an embedded secure processor 110 (and possibly other processors).

In one embodiment, content 131 or license information 141 received by the secure processor 110 or the playback device 120 might be maintained on the external storage 112, digitally encrypted against discovery and digitally signed against tampering using a

public/private key pair in a public key cryptosystem, the public/private key pair being maintained in the internal storage 111.

The content server 130 includes a set of content 131 suitable for execution or presentation. The content 131 can be distributed to the secure processor 110 or the playback device 120, using an electronic form of delivery (such as for example a broadcast technique or a computer network), a physical form of delivery (such as for example transport of physical media on which the content 131 is embedded in an encoded format), or some other form of distribution by which the secure processor 110 or the playback device 120 receives the content 131 in a relatively economical manner.

The license server 140 includes a processor, program and data memory, capable of receiving request messages 141 for one or more of a set of licenses 142, capable of generating or retrieving licenses 142, and capable of sending response messages 143 including information relating to those licenses 142.

Although it is possible for the secure processor 110 or the playback device 120 to communicate directly with the license server 140, in one embodiment, the secure processor 110 and the playback device 120 need not have any connection to the communication link 160. In such embodiments, the user 150 obtains information, if such information is necessary to request a license 142, from the secure processor 110 or the playback device 120. The user 150 generates a request message 141 including information necessary to request the license 142, and sends that request message 141 to the license server 140, without the assistance of either the secure processor 110 or the playback device 120.

In one embodiment, the user 150 reads a first alphanumeric or numeric code 151 from the output element 121 of the playback device 120, including information sufficient to generate a request message 141 that can be sent to the license server 140. For a first example, not intended to be limiting in any way, the first alphanumeric or numeric code might include a hexadecimal representation of the request message 141. For a second example, not intended to be limiting in any way, the first alphanumeric or numeric code 151 might include instructions to the user 150 to read the information sufficient to generate a request message 141 from another source, such as for example a first unique identifier

imprinted on the playback device 120 and a second unique identifier imprinted on physical media (such as for example a CD or DVD) on which the content 131 is embedded.

In one embodiment, the user 150 uses a communication device 152, such as for example a cellular telephone, a "Palm Pilot" or PDA or other hand-held computer, or a hybrid thereof, capable of communication using the SMS (short message service) protocol, to send the request message 141 to the license server 140. In such embodiments, the communication link 160 between the license server 140 and the user 150 includes a private or public switched telephone network including cellular telephony. However, as described below, other and further examples of communication between the license server 140 and the user 150 are within the scope of the invention, with the effect that the communication link 160 might include one of a wide variety of techniques for transporting information from the user 150 to the license server 140, and back from the license server 140 in response thereto.

The SMS protocol is a relatively low data rate protocol using GSM wireless networks. SMS is supported by many makes and models of cellular telephones, hand-held computers, and similar devices. The license server 140 receives the request message 141, generates a license 142 (in response to information recoverable from that request message 141), and sends a response message 143 (including information sufficient to recover the license 142) to the user 150. In one embodiment, the user 150 receives the response message 143 at the same communication device 152, but in the context of the invention, this is not a requirement.

In one embodiment, the user 150 reads the response message 143 from the communication device 152 (SMS is a text-based protocol, so the response message 143 should be readable by a human user 150). The user 150 enters at least some information from the response message 143 into the input console 122, with the effect that the secure processor 110 and the playback device 120 are able to receive that information without having any direct communication link to the license server 140.

After reading this application, other and further examples of communication between the license server 140 and the user 150 would be clear to those skilled in the art. After reading this application, those skilled in the art would recognize that such other and

further examples would be workable in response to information from this application, are within the scope of the invention, and would not require undue experiment or further invention. Such other and further examples include:

- Examples of immediate payment: credit or debit cards, pre-paid phone cards, scratch-off phone cards, telephone billing using 900 or 976 phone numbers, vending devices taking deposits of actual bills, coins, or tokens.

- Examples of non-immediate payment: account numbers with credits or debits, subscription accounts. Any of these could use either cash or game credits.

- Examples of other types of communication to request licenses: Palm Pilot communication using digital ink or handwriting recognition, Palm Pilot communication using stylus gestures, telephone calls using touch tone and AVR (automated voice response), telephone calls using voice recognition.

- Examples of other types of communication to respond with license information: a broadcast or cablecast message direct to the secure processor or the playback device, or a web server returning an activation code in response to appropriate input request, such as possibly using a hypertext protocol.

- Examples of other types of recognition of the playback device: Bluetooth recognition of the playback device from the cellular telephone, GPS location of the user.

In one embodiment, the secure processor 110 and the playback device 120 are coupled to a LAN (local area network) or a secure enterprise network, with the effect that the secure processor 110 and the playback device 120 can communicate with other such secure processors 110 or playback devices 120 without any requirement for a communication link 160 capable of relatively remote communication.

Method of Operation

Figure 2 shows a process flow diagram of a method of using a system including a closed distribution system and a separate connection capable of delivery of license information or activation code.

Although described serially, the flow points and steps of the method 200 can be performed by separate elements in conjunction or in parallel, whether asynchronously or synchronously, in a pipelined manner, or otherwise. In the context of the invention, there is no particular requirement that the method 200 must be performed in the same order in which this description lists flow points or steps, except where explicitly so indicated.

At a flow point 210A, the system 100 is ready to deliver content 131 to the secure processor 110 or playback device 120, and to make that content 131 available to the user 150 for execution by the secure processor 110 or presentation by the playback device 120.

At a step 211, the secure processor 110 or the playback device 120 receives content 131 from the content server 130.

At a step 212, the user 150 indicates a desire to use the content 131 received from the content server 130.

At a step 213, either the secure processor 110 or the playback device 120 provides sufficient information for the user 150 to request a license 142 from the license server 140.

At a step 214, the user 150 uses the communication link 160 to obtain a license 142 from the license server 140. As part of this step, the user performs the following sub-steps:

- At a sub-step 214(a), the user 150 copies the information obtained above in the step 213 to the communication device 152.

- At a sub-step 214(b), the communication device 152 generates a request message 141 for a license 142. In one embodiment, the request message 141 includes a proof of payment by the user 150 for the license 142, such as an account number to charge or verify, a credit or debit card number to charge, a code derived from a scratch-off card, and the like, as described above with regard to figure 1.

- At a sub-step 214(c), the license server 140 receives the request message 141.

- At a sub-step 214(d), the license server 140 determines if the user 150 should be granted a license 142. If not, the license server 140 generates a response message 143 denying the license, and the method 200 returns to the flow point 210A. In one embodiment, as part of determining if the user 150 should be granted a license 142, the license server 140 authenticates the proof of payment by the user 150 for the license 142.

- At a sub-step 214(e), the license server 140 generates a license 142 for the specific playback device 120 and the specific user 150.

- At a sub-step 214(f), the license server 140 sends a response message 143 including information from which the playback device 120 can recover the license 142.

- At a sub-step 214(g), the user 150 receives the response message 143 and enters information from that message using the input console 122.

At a step 215, the secure processor 110 and the playback device 120 verify that the license 142 is authentic, and that the license 142 grants rights for the specific user 150 to use the specific content 131 with the specific playback device 120.

At a step 216, the secure processor 110 maintains information relating to the license 142, including the rights granted to the specific user 150, in secure storage (either the internal storage 111 or, subject to digital encryption and digital signature, the external storage 112).

At a step 217, the secure processor 110 and the playback device 120 execute or present the content 131, subject to the rights granted by the license 142. In one embodiment, execution or presentation might be interactive with the user 150.

At a flow point 210B, the system 100 has delivered content 131 to the secure processor 110 or playback device 120, and made that content 131 available to the user 150 for execution by the secure processor 110 or presentation by the playback device 120, and is now ready to perform another task.

Alternative Embodiments

Although preferred embodiments are disclosed herein, many variations are possible which remain within the concept and scope of the invention. These variations would become clear to those skilled in the art after perusal of this application.

- A license requesting device could automatically make the request with its embedded ID. This might be the playback device itself.

- The content ID might be implicitly assumed, since there is only one application for which rights are purchased.

- The rights might be in terms of duration of execution or number of times of execution (for example, MP3 sound recordings), with licenses being generic or specific to a particular content identifier.

- The method of authentication or verification of the license might include the following: The license server might deliver a content key for the specific encrypted content, in turn encrypted by a shared secret key known only to the specific player. This ensures that only the intended recipient is able to play the content.

- The method of authentication or verification of the license might include the following: The license server might deliver a signature over a token including the player and content identities. The security software is able to enforce the check

against its own identity and the content identity. In lieu of the signature, the server could (either in addition or instead) encrypt the token using a shared key known only to the intended recipient.

After reading this application, those skilled in the art would recognize that the techniques described herein provide an enabling technology, with the effect that heretofore advantageous features can be provided that heretofore were substantially infeasible. After reading this application, those skilled in the art will recognize that these alternative embodiments and variations are illustrative and are intended to be in no way limiting.

Claims

1. A method including steps of

sending a text-based message to a hand-held device using an SMS technique, the text-based message including information from which rights information is derivable by a system including a playback device; and

enforcing that rights information on the system in response to that text-based message;

wherein the steps of sending include a transport technique not including the playback device.

2. A method as in claim 1, including steps of ensuring that only authorized content is executed or presented by the playback device or the secure processor, or by both in combination or conjunction.

3. A method as in claim 1, including steps of sending content to the playback device using a communication link not used by the steps of sending a text-based message.

4. A method as in claim 1, wherein the steps of enforcing are performed at least in part by the playback device or a secure processor coupled thereto.

5. A method as in claim 1, wherein the steps of enforcing are performed by mandatory security hardware or mandatory security software.

6. A method as in claim 1, wherein the steps of enforcing include steps of decrypting at least some information derivable from the text-based message.

7. A method as in claim 1, wherein the steps of enforcing includes using a key derived from the message for decrypting a license or content.

8. A method as in claim 1, wherein the steps of enforcing includes applying a key derived from the message to complete a license in which execution rights are defined.

9. A method as in claim 1, wherein the steps of enforcing includes applying a key derived from the message as an authentication code.

10. A method as in claim 1, wherein the message is composed on the SMS.

11. A method as in claim 1, wherein the message is manually entered into the playback device.

12. A method as in claim 11, wherein the playback device processes the message and produces a licensing message suitable to be sent by the handheld device.

13. A method as in claim 12, wherein the licensing message is encrypted or cryptographically authenticated by the handheld device and sent to a license server.

14. A method as in claim 1, wherein the steps of enforcing include steps of using a decryption key available to the by the playback device or a secure processor coupled thereto.

15. A method as in claim 1, wherein the steps of sending a text-based message include steps of sending a first message from a hand-held device using an SMS technique to a license server;

sending a second message from the license server to the hand-held device, the second message including human-readable characters; and

manually entering those characters to an input element coupled to the playback device.

16. A method as in claim 1, wherein the system includes a closed content distribution system capable of delivering content to the playback device using a second transport technique not including that used by the steps of sending a text-based message.

17. A method as in claim 1, wherein the system includes a closed content distribution system capable of ensuring that only authorized content is presented by the playback device or executed by the secure processor.

18. A method as in claim 1, wherein the text-based message includes an authentication code; and

the system includes a secure processor capable of authenticating content coupled to the playback device in response to that authentication code.

19. A method as in claim 1, including steps of authenticating the right information by the playback device or a secure processor coupled thereto.

20. A method as in claim 19, wherein the steps of authenticating include steps of decrypting at least some information derivable from that text-based message.

21. A method as in claim 19, wherein the steps of authenticating include steps of using a decryption key available to the by the playback device or a secure processor coupled thereto.

22. A method as in claim 1, including steps of

decoding those characters; and

deriving rights information from at least some of those characters.

23. A method as in claim 22, wherein the steps of deriving are performed at least in part by the playback device or a secure processor coupled thereto.

24. A method as in claim 22, wherein those characters include at least some information encrypted using a key available to the playback device or a secure processor coupled thereto.

25. A method including steps of

sending a text-based message to a hand-held device using an SMS technique, the text-based message including information from which rights information is derivable by a system including a playback device including at least one of rights-enforcing hardware, rights-enforcing software;

enforcing that rights information on the system using the rights-enforcing hardware or rights-enforcing software, in response to that text-based message.

26. A method as in claim 25, including steps of authenticating that rights information using the rights-enforcing hardware or rights-enforcing software.

27. A method including steps of

sending a text-based message to a hand-held device using an SMS technique, the text-based message including information from which rights information is derivable by a system including a secure processor and a playback device under control of that secure processor;

authenticating that rights information at the secure processor in response to mandatory security software executed by the secure processor; and

enforcing that rights information on the system in response to that text-based message.

28. A method as in claim 27, including steps of sending content to the playback device using a communication link not used by the steps of sending a text-based message.

29. A method as in claim 27, wherein the steps of sending a text-based message include a transport technique not including the playback device.

30. A method as in claim 27, wherein the steps of sending a text-based message include steps of

sending a first message from a hand-held device using an SMS technique to a license server;

sending a second message from the license server to the hand-held device, the second message including human-readable characters; and

entering those characters to an input element coupled to the secure processor.

31. A method as in claim 27, wherein the system includes a closed content distribution system capable of delivering content to the playback device using a second transport technique not including that used by the steps of sending a text-based message, the closed content distribution system including the mandatory security software being responsive to a private key in a public-key cryptosystem.

32. A method as in claim 27, wherein the system includes a closed content distribution system capable of ensuring that only authorized content is presented by the playback device or executed by the secure processor.

33. A method as in claim 27, wherein

the text-based message includes an authentication code; and

the system includes a secure processor capable of authenticating content coupled to the playback device in response to that authentication code.

34. A method including steps of

sending a text-based message to a hand-held device using an SMS technique, the text-based message including information from which rights information is derivable by a system including a playback device under control of a secure processor;

enforcing that rights information at the secure processor; and

at least one of the steps of

(A) decrypting data by the secure processor in response to a secret key and without exposing that secret key, and

(B) authenticating that rights information in response to mandatory security software executed by the secure processor.

35. A method including steps of

sending a text-based message to a hand-held device using an SMS technique, the text-based message including information from which rights information is derivable by a system including a playback device under control of a secure processor; and

enforcing that rights information at the secure processor;

wherein the steps of enforcing that rights information include one or more of the steps of

(A) the secure processor receiving a decryption key for content delivered to the playback device, the decryption key being itself encrypted using a private key available only to the secure processor,

(B) the secure processor authenticating that rights information in response to a digital signature or secure hash thereof,

(C) the secure processor receiving a shared key for rights information delivered to the secure processor, and the secure processor authenticating that rights information in response to that shared key, and

(D) the secure processor receiving a shared key for content delivered to the playback device, and the secure processor authenticating that content in response to that shared key.

36. A method including steps of delivering license information in a closed content distribution system, the closed content distribution system including a playback device and a secure processor, the steps of delivering including a communication link not including the playback device or secure processor, the communication link including a short text-messaging system;

ensuring that only authorized content is executed or presented by the playback device or the secure processor, or by both in combination or conjunction; and

ensuring that rights information derivable from the license information is enforced by the playback device or the secure processor, or by both in combination or conjunction.

37. A method as in claim 36, including steps of authenticating the license information by the playback device or the secure processor, or by both in combination or conjunction.

38. A method as in claim 36, including steps of determining in response to the rights information whether the user is authorized to execute or present the selected content.

39. A method as in claim 36, including steps of encoding the license information using a digital signature, secure hash, or shared secret; and

authenticating the license information by the playback device or the secure processor, or by both in combination or conjunction, in response to the digital signature, secure hash, or shared secret.

40. A method as in claim 36, including steps of receiving content at the playback device.

41. A method as in claim 36, wherein at least a portion of the content is included on physical media transported to the playback device or secure processor.

42. A method as in claim 36, wherein at least a portion of the content is present at the playback device or secure processor before the steps of delivering license information.

43. A method as in claim 36, wherein the communication link includes a cellular telephone.

44. A method as in claim 36, wherein the content can be executed or interpreted by the playback device or the secure processor, or by both in combination or conjunction.

45. A method as in claim 36, wherein the content can be presented in a human-sensible form by the playback device or the secure processor, or by both in combination or conjunction.

46. A method as in claim 36, wherein the secure processor includes a computing device capable of enforcing mandatory execution of selected security software.

47. A method as in claim 36, wherein the secure processor includes a computing device capable of general purpose processing.

48. A method as in claim 36, wherein the steps of delivering include steps of sending a text-based message to a hand-held device using an SMS technique, the text-based message including information from which rights information is derivable.

49. A method as in claim 36, wherein the steps of ensuring include steps of decoding the license information;

generating at least a portion of the rights information in response to the steps of decoding; and

enforcing the rights information.

50. A method as in claim 36, including steps of performing a commercial transaction concurrently with communication between the license server and the user.

51. A method as in claim 50, wherein the steps of performing a commercial transaction include steps of receiving information at the license server sufficient to allow that license server to effect a purchase transaction by the user.

52. A method as in claim 50, wherein the steps of performing a commercial transaction include steps of receiving proof of purchase at the license server of a license by the user.

53. A method as in claim 36, including steps of performing mandatory security software by the secure processor.

54. A method as in claim 53, wherein the steps of performing mandatory security software include one or more of:

authenticating at least one of: a specific content element, a specific playback device or secure processor, a specific user;

enforcing comparison of an identity associated with the playback device with a tamper-proof identity available to the playback device or the secure processor, or to both in combination or conjunction;

enforcing comparison of rights information with an identity of selected content available to the playback device or the secure processor, or to both in combination or conjunction;

enforcing computation of the secret key (using its private key and server public key) and decryption of the identities; and

enforcing verification of a signature by the license server.

55. A method as in claim 36, wherein the steps of delivering include steps of delivering a code from a license server to a user; and

manually communicating the code from the user to the playback device or the secure processor.

56. A method as in claim 55, including steps of deriving license information from the code.

57. A method as in claim 55, including steps of decrypting content in response to the code.

58. A method as in claim 55, wherein the code includes a human-readable alphabetic, alphanumeric, numeric, or other character string.

59. A method as in claim 55, wherein the code includes a representation of at least a portion of a license message.

60. A method as in claim 55, wherein the steps of communicating the code include a human input device.

61. A method as in claim 55, wherein the steps of communicating the code include an input technique not part of the closed distribution system.

62. A method as in claim 55, wherein the steps of communicating the code include an SMS protocol.

63. A method as in claim 55, wherein the steps of communicating the code include a text messaging protocol.

64. A method as in claim 55, wherein the code includes a representation of a content decryption key.

65. A method as in claim 64, wherein the closed distribution system includes a public-key cryptosystem; and

the content decryption key includes a decryption key privately associated with the content, encrypted by an encryption key publicly associated with a specific playback device.

66. A method as in claim 55, wherein the code includes a representation of an identifier of one or more of: a specific content element, a specific playback device or secure processor, and a specific user.

67. A method as in claim 66, including steps of authenticating the code, the steps of authenticating including one or more of:

determining if the code is digitally signed by a license server; and

determining if the code is encrypted by a key known commonly to both the license server and the specific user.

68. A method as in claim 66, including steps of authenticating the code, the steps of authenticating including one or more of:

determining if the code is digitally signed by a license server; and

determining if the code is encrypted by a key known commonly to both the license server and the specific playback device or secure processor, or both in combination or conjunction.

69. Apparatus including a closed content distribution system including

a playback device and a secure processor;

a communication link not including the playback device or secure processor;

a license server capable of being coupled to the communication link;

wherein the playback device or the secure processor, or both in combination or conjunction, includes mandatory security software.

70. Apparatus as in claim 69, wherein at least a portion of the content is included on physical media transported to the playback device or secure processor.

71. Apparatus as in claim 69, wherein the communication link includes a cellular telephone.

72. Apparatus as in claim 69, wherein the mandatory security software includes instructions authenticating the license information.

73. Apparatus as in claim 69, wherein the mandatory security software includes instructions determining in response to the rights information whether the user is authorized to execute or present the selected content.

74. Apparatus as in claim 69, wherein the mandatory security software includes instructions of

encoding the license information using a digital signature, secure hash, or shared secret; and

authenticating the license information by the playback device or the secure processor, or by both in combination or conjunction, in response to the digital signature, secure hash, or shared secret.

75. Apparatus as in claim 69, wherein

the mandatory security software includes instructions ensuring that only authorized content is executed or presented by playback device or the secure processor, or both in combination or conjunction; and

rights information derivable from the license information is enforced by the playback device or the secure processor, or by both in combination or conjunction.

76. Apparatus as in claim 69, wherein the mandatory security software includes one or more of:

instructions authenticating at least one of: a specific content element, a specific playback device or secure processor, and a specific user;

instructions enforcing comparison of an identity associated with the playback device with a tamper-proof identity available to the playback device or the secure processor, or to both in combination or conjunction;

instructions enforcing comparison of rights information with an identity of selected content available to the playback device or the secure processor, or to both in combination or conjunction;

instructions enforcing computation of the secret key (using its private key and server public key) and decryption of the identities; and

instructions enforcing verification of a signature by the license server.

77. Apparatus as in claim 69, wherein the secure processor includes a computing device capable of general purpose processing.

78. Apparatus as in claim 69, including a code delivered from a license server to a user, the code being communicated from the user to the playback device or the secure processor.

79. Apparatus as in claim 78, including a content decryption key embedded in the code.

80. Apparatus as in claim 78, including a human input device coupled to the playback device or the secure processor.

81. Apparatus as in claim 78, including license information embedded in the code.

82. Apparatus as in claim 78, including an SMS protocol message.

83. Apparatus as in claim 78, including a text messaging protocol message.

84. Apparatus as in claim 78, wherein the code includes a human-readable alphabetic, alphanumeric, numeric, or other character string.

85. Apparatus as in claim 78, wherein the code includes a representation of at least a portion of a license message.

86. Apparatus as in claim 78, wherein the code includes a representation of a content decryption key.

87. Apparatus as in claim 86, wherein

the closed distribution system includes a public-key cryptosystem; and

the content decryption key includes a decryption key privately associated with the content, encrypted by an encryption key publicly associated with a specific playback device.

88. Apparatus as in claim 78, wherein the code includes a representation of an identifier of one or more of: a specific content element, a specific playback device or secure processor, and a specific user.

89. Apparatus as in claim 88, wherein the mandatory security software includes instructions authenticating the code, the instructions including one or more of:

instructions determining if the code is digitally signed by a license server; and

instructions determining if the code is encrypted by a key known commonly to both the license server and the specific user.

90. Apparatus as in claim 88, wherein the mandatory security software includes instructions authenticating the code, the instructions including one or more of:

instructions determining if the code is digitally signed by a license server; and

instructions determining if the code is encrypted by a key known commonly to both the license server and the specific playback device or secure processor, or both in combination or conjunction.

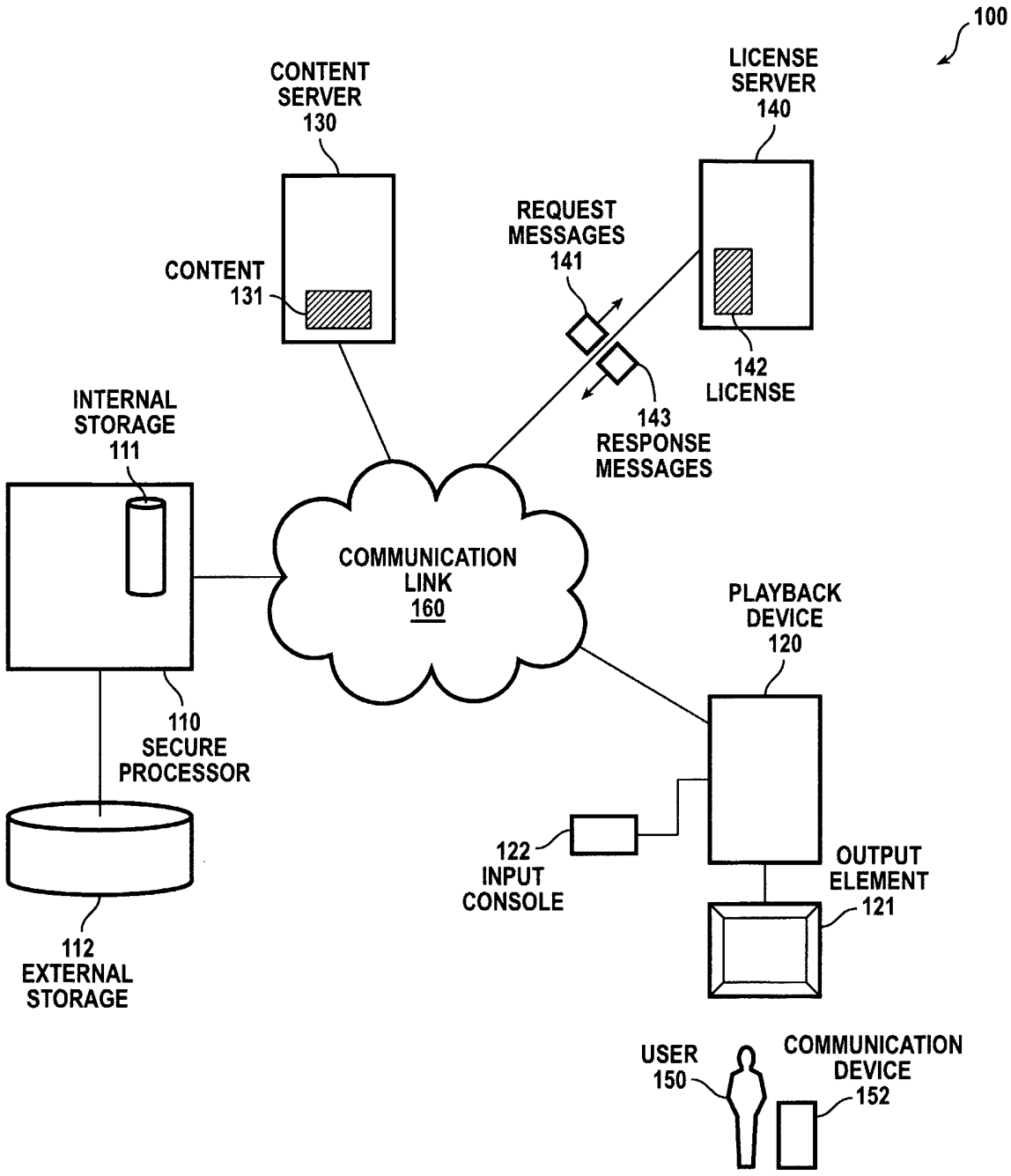

100
CONTENT SERVER 130
LICENSE SERVER 140
CONTENT 131
REQUEST MESSAGES 141
142 LICENSE
143 RESPONSE MESSAGES
INTERNAL STORAGE 111
COMMUNICATION LINK 160
PLAYBACK DEVICE 120
110 SECURE PROCESSOR
122 INPUT CONSOLE
OUTPUT ELEMENT 121
112 EXTERNAL STORAGE
USER 150
COMMUNICATION DEVICE 152

FIG. 1

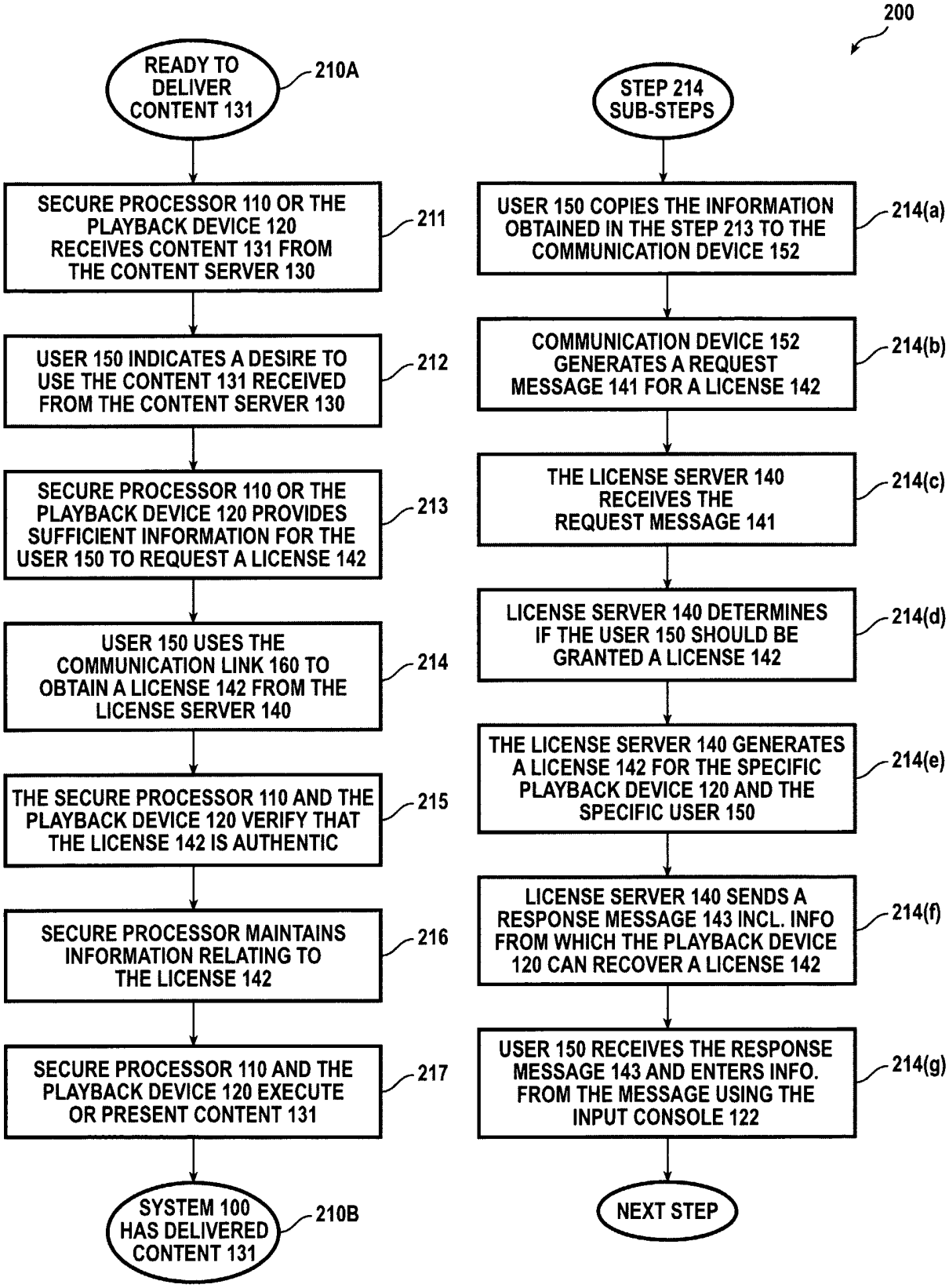

200
READY TO DELIVER CONTENT 131
210A
SECURE PROCESSOR 110 OR THE PLAYBACK DEVICE 120 RECEIVES CONTENT 131 FROM THE CONTENT SERVER 130
211
USER 150 INDICATES A DESIRE TO USE THE CONTENT 131 RECEIVED FROM THE CONTENT SERVER 130
212
SECURE PROCESSOR 110 OR THE PLAYBACK DEVICE 120 PROVIDES SUFFICIENT INFORMATION FOR THE USER 150 TO REQUEST A LICENSE 142
213
USER 150 USES THE COMMUNICATION LINK 160 TO OBTAIN A LICENSE 142 FROM THE LICENSE SERVER 140
214
THE SECURE PROCESSOR 110 AND THE PLAYBACK DEVICE 120 VERIFY THAT THE LICENSE 142 IS AUTHENTIC
215
SECURE PROCESSOR MAINTAINS INFORMATION RELATING TO THE LICENSE 142
216
SECURE PROCESSOR 110 AND THE PLAYBACK DEVICE 120 EXECUTE OR PRESENT CONTENT 131
217
SYSTEM 100 HAS DELIVERED CONTENT 131
210B
STEP 214 SUB-STEPS
USER 150 COPIES THE INFORMATION OBTAINED IN THE STEP 213 TO THE COMMUNICATION DEVICE 152
214(a)
COMMUNICATION DEVICE 152 GENERATES A REQUEST MESSAGE 141 FOR A LICENSE 142
214(b)
THE LICENSE SERVER 140 RECEIVES THE REQUEST MESSAGE 141
214(c)
LICENSE SERVER 140 DETERMINES IF THE USER 150 SHOULD BE GRANTED A LICENSE 142
214(d)
THE LICENSE SERVER 140 GENERATES A LICENSE 142 FOR THE SPECIFIC PLAYBACK DEVICE 120 AND THE SPECIFIC USER 150
214(e)
LICENSE SERVER 140 SENDS A RESPONSE MESSAGE 143 INCL. INFO FROM WHICH THE PLAYBACK DEVICE 120 CAN RECOVER A LICENSE 142
214(f)
USER 150 RECEIVES THE RESPONSE MESSAGE 143 AND ENTERS INFO. FROM THE MESSAGE USING THE INPUT CONSOLE 122
214(g)
NEXT STEP

FIG. 2