

A METHOD AND APPARATUS FOR DELIVERING KEYS

Claim of Priority under 35 U.S.C §119

[0001] The present Application for Patent claims priority to U.S Provisional Application No. 60/588,203, entitled, "A Method And Apparatus For Delivering Keys," filed on July 14, 2004, and assigned to the assignee hereof and expressly incorporated by reference herein.

FIELD OF THE INVENTION

[0002] This invention relates to the field of content delivery system, and in particular to the delivery and reception of keys between a server and one or more client terminals.

BACKGROUND OF THE INVENTION

[0003] In a content delivery system, operating in a wireless communication that utilizes a portable client and fixed server for delivery of audio and video content, protection and management of digital rights are a concern. Various methods are employed to efficiently deliver content such that digital rights of the content owner are protected. One conventional way to manage and protect the digital rights is to encrypt the content at the server using one or more keys (encryption or decryption) and providing the keys to an authorized user, using a client device, who subscribes to the content. Thus, the users with keys may decrypt the content to view and/or listen to subscribed content.

[0004] Generally, content is encrypted using keys (one or more bits) and the keys are delivered on a regular basis. The keys that decrypt the content are delivered periodically. In order to provide the content and keys that decrypt the content at client devices, various over the air techniques are used. Often, a key-exchange method is employed to provide a set of keys (for example public keys and private keys) between the server and the client.

[0005] A common method is for the client to request a new key(s) or server sending new key(s) to the client. According to this method, a new connection is made between client and server in order to transmit the keys to client. Depending on time of day, there could be several client devices on the system,

each requesting a new set of keys. Responsive to the key requests, a new connection must be opened to exchange the keys. Most systems today require that new keys be used each time a new content is provided to the user, since using new keys provide a greater security. Also, each time one or more keys expire or each time a subscription is renewed, a new connection is created to update old or expired keys. This is a burden on system, considering that there are thousands of devices that may request access to new content or renew subscription. Opening and closing a connection ties up resources for the server, especially during peak hours. It would be useful to exchange keys without having to create a new connection and get the necessary keys to the client.

[0006] Therefore, an efficient delivery system is needed to deliver keys without placing an extra burden on the content delivery system.

SUMMARY OF THE INVENTION

[0007] An embodiment of invention provides an apparatus and an associated method, for an electronic device, that manages delivery of one or more keys to another electronic device without creating unnecessary connections between the server and the mobile terminal.

[0008] The exemplary electronic device, such as a server, may be operated in a communication system (for example CDMA, TDMA, GSM, OFMD, OFDMA etc.). The electronic device comprises a method for receiving a request from another electronic device to transmit keys, for example a mobile terminal. Responsive to the request, the server generates the required keys and determines a best time to send the keys to the mobile client device such that a new connection is not required just for sending the requested keys. The best time to send the keys may be during a scheduled connection for sending non-key data, for example a connection setup for transmitting system parameters, content data, etc. By sending the keys along with the non-key data, a need for a special connection is avoided.

[0009] The embodiment also encompasses an electronic device, such as mobile terminal, which may be operated in a communication system (for example CDMA, TDMA, GSM, OFDM, OFDMA etc.). The mobile terminal comprises a method for requesting one or more keys from a server and

receiving the requested keys during a connection setup by the server for transmitting non-key data. By receiving the keys along with non-key data, need for a special connection is avoided.

[0010] The embodiment also encompasses an electronic device, such as mobile device, a server computer, portable computer, etc. operable in a communication system. The server computer comprises a method for receiving a request for one or more keys from an external electronic device and transmitting the requested keys during a connection setup for transmitting non-key data. By transmitting the keys along with non-key data, a need for a special connection is avoided.

[0011] A more complete appreciation of all the embodiments and scope can be obtained from the accompanying drawings, the following detailed description of the invention, and the appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] Figure 1 illustrates a block diagram of electronic devices operating in wireless content delivery system according to an embodiment of the invention;

[0013] Figure 2A illustrates an example of operation of content delivery system using key epochs;

[0014] Figure 2B illustrates an example of operation of content delivery system during a key epoch;

[0015] Figure 3 illustrates an example of flowchart of tasks performed by processor of the server device according to an embodiment the invention; and

[0016] Figure 4 illustrates an example of flowchart of tasks performed by processor of the mobile client device according to an embodiment the invention.

DETAILED DESCRIPTION OF THE INVENTION

[0017] Figure 1 illustrates a communication system and block diagram of electronic devices operating within the system, such as a server device 100, mobile client terminal 122 ("Client") and content provider 120. The server device 100 comprises a controller (which may also be known as processor 102 and may control the operations of the server device 100) coupled to memory 103

and various servers (collectively known as core network 105). Each of the various servers may comprise a processor, receiver, transmitter and various memories and may also be coupled to processor 102, memory 103, transmitter 104 and receiver 107. Generally, the server device 100 receives content from the content provider 120 and the server device communicates with one or more mobile client terminals 122. The server device 100 may be a stand alone computer or a plurality of computers connected each other to form server device 100. The server device 100 may also be a mobile terminal wirelessly connected to the one or more computers and one or more mobile client terminal 122.

[0018] The core network 105 includes a distribution center 111 comprising a content server 112 which receives content for the system directly from the content provider 120, a distribution server 114 distributes the content to one or more mobile client devices, and a program content database 118 stores content received from the content provider 120. The core network may comprises a digital rights management server (DRM) 106 that generates one or more keys (for example general keys for decryption, program keys, session keys, encrypted program keys, service keys and service licenses) and manages the secure storage of those keys. Subscription server 108 performs subscription management for the system and communicates to mobile client device. A License Key server (LKS) 110 services key requests from the subscribed mobile client terminals 122, and an Overhead Notification server (ONS) 116 is responsible for collecting notifications of state changes which are timely transmitted to the mobile client terminal 122. The transmitter 104 and the receiver 107 are coupled to the processor 102. It should be noted that transmitter 104 and receiver 107 may be connected wirelessly or by hard wire to external devices for transmitting and receiving information, respectively.

[0019] The example of mobile client terminal 122 comprises a controller (which may also be referenced to as processor 126) coupled to memory 127. The mobile client terminal 122 communicates with the server device 100 to receive content and keys to decrypt the content.

[0020] FIG. 2A and 2B illustrates an example of operation of content delivery system using key epochs 200 and various messages that are sent between the sever device 100 and the mobile device 122. An epoch is a unique period of

time wherein a specific key is valid. Generally, a time period, for example a 24-hour period, is divided in to one or more key epochs. The length of the each key epoch that may be predetermined by the system provider or dynamically configurable. FIG. 2A shows an example of key epoch T1 202 and key epoch T2 204, and an example of operation of the content delivery system during the epochs. In a typical content delivery system, the server device 100 is not always connected to the mobile client terminal 122. Based on the service provider, the server device 100 only periodically communicates with one or more mobile client terminals to reduce congestion in the system. Service providers generally do not have enough bandwidth to communicate with all the mobile client terminals on an "Always-On" basis. Therefore, most service providers schedule a time to open a connection, for example a connection window for sending and receiving data between mobile client terminal 122 and server device 100.

[0021] As shown in FIG 2A, key epoch T1 202 further comprises a delta portion 206, which is $T2 - X$, wherein X represents a time change (delta) before the start of T2 204 epoch. Preferably, during this time, the system attempts to create a connection between the server device 100 and one or more of mobile client terminal 122 in the system. The connection (also known as a communication link) is made during one or more scheduled windows, for example 208, 210 and 212. The communication link may be made using various known wireless communication techniques, for example CDMA 1X-EVDO system or Orthogonal Frequency Divisional Multiple Access (OFDMA) system, that allow transmission and reception of multi-media data. The operators of the system may decide the value of X, which will affect the size of the delta 206 and number of windows that can be created during this time. Also, depending on the operator and the type of information that is need to be communicated, a window of time may communicated with one mobile client terminal 122 or several mobile client terminals at the same time. Therefore, several hundred windows may be used to ensure that necessary or requested information is sent to the mobile client terminals.

[0022] As shown in FIG. 2B, prior to the start of a scheduled window, for example 208, an epoch event 214 is created. Thereafter, a communication link between the server device 100 and the mobile client terminal 122 is created.

Information for the start of the window period and setting up the communication link is sent to the mobile client terminal 122. Message 216 is used to communicate information, such as system parameters that set up the communication link. The server device 100 schedules a time when message 216 is sent to the mobile client device 122. Typically, message 216 contains only non-key data; however, it is contemplated that message 216 may also contain key data. Non-key data is any data other than encryption or decryption keys (example portion of decryption key, program key, session key, etc). For example, non-key data may be data representing content, program application, or executable code. The non-key data may also comprise set of system parameters comprising a data rate information of the communication link, server device states, status of keys and program content. Responsive to receiving message 216, the mobile client terminal 122 may send a message 218 to request for new content or/and keys for future use. If the mobile client terminal 122 has requested new keys, then the server device 100 will generate new keys by communicating with the digital rights management (DMR) server device 100 using 220 and 222 messages. Thereafter, message 224 is generated and transmitted to mobile client device 122. Generally, message 224 is a scheduled for transmitting non-key data only, unless the requested keys are ready to be transmitted during this window.

[0023] According to an embodiment, the server device 100 may take advantage of the transmission of the messages 216 or 224 to send one or more keys. Generally, message 216 and 214 are not intended to send any keys, only system parameters. If the server device 100 has any keys to transmit to the mobile client terminal 122, then the server device 100 may attach the keys during these transmissions to avoid having to create a new connection for transmitting the keys. Also, if determined through message 218 that the mobile client terminal 122 needs new keys then the server device 100 may take advantage of sending keys along with non-key data message 224 to transmit keys to the mobile client terminal 122, without creating a special connection.

[0024] Figure 3 illustrates an example of flowchart 300 of tasks of delivering keys is performed by processor 102 of the server device's 100 according an embodiment the invention. At block 302, data is continually being prepared for

transmission. At block 304, the processor processing a scheduled event to send a message to the external device. At block 306, the processor creating a non-key data message to be sent to one or more mobile client terminals; typically this message only contains system parameters to create a connection. At block 308, the processor determining if there are any keys that need to be sent to at least one or more mobile client terminals in the system. If yes, then at block 310, the processor attaching the keys to this message, a scheduled non-key data message, and transmits the message. Otherwise, at block 312, transmitting the non-key data message without any keys. Responsive to the transmitted message of block 310 or 312, at block 314 the processor receiving a response from the mobile client terminal 122. Generally, this response establishes a connection between the server device 100 and mobile client terminal 122. At block 316, the processor determining if the mobile client terminal received the keys sent at block 310, or determining if the mobile client terminal is requesting new keys. At block 318, the processor processing the response received from the mobile client terminal 122 to determine if the transmitted keys were received by the mobile client terminal 122. If yes, then at block 320, processor determining if the mobile client terminal 122 has requested new keys. If yes, then at block 322, the processor generating the necessary keys and at block 324, attaching the keys to the next scheduled message communicated to the mobile client terminal 122. Otherwise, processor returns to block 302. If determined that at block 318 that the keys were not received, then at block 324, attaching the keys to the next scheduled message communicated to the mobile client terminal 122.

[0025] Figure 4 illustrates an example of flowchart 400 of tasks performed by the mobile client terminal's 122 processor 126 for receiving keys according to an embodiment of the invention. At block 402, the mobile client terminal 122 is an idle state of the content delivery system wherein, the server device 100 and the mobile client terminal 102 may have a communication link or may have communication link without data connection. The mobile client terminal 122 is waiting for communication from the server device 100. At block 404, the processor processing a received message, generally from the server device 100. This message may or may not contain any keys. At block 406, the processor

determining if the received message contained any keys. If yes, then at block 408, the processor 126 extracting one or more keys, processing the extracted keys and then storing the keys in a database. Thereafter at block 408, receiving one or more keys during a connection scheduled for receiving non-key data. At block 410, the processor 126 determining if the mobile client terminal 122 will need new keys. If so, then at block 412, the processor 126 will notifying the server device 100 or requests the new keys. Thereafter, the processor waits at block 402 for another message from the server device 100 to extract the keys.

[0026] As examples, the method and apparatus may also be implemented in mobile electronic devices such as a mobile telephone, PDA, mobile computers, mobile server computer and other devices having a wireless connection system and receiving audio and video data. Also, as example, the content may by block of video and audio data such as full television program or segment of one or more program.

[0027] While the invention has been particularly shown and described with reference to a preferred embodiment, it will be understood by those skilled in the art that various changes in form and details may be made therein without departing from the scope of the invention as defined by the appended claims. That is, other modifications and variations to the invention will be apparent to those skilled in the art from the foregoing disclosure and teachings. Thus, while only certain embodiments of the invention have been specifically described herein, it will be apparent that numerous modifications may be made thereto without departing from the spirit and scope of the invention.

What is claimed is:

CLAIMS

1. A method of receiving one or more keys, the method comprising acts of:
determining whether to request said one or more keys;
requesting delivery of said one or more keys; and
receiving said one or more keys during a connection scheduled for receiving a non-key data.
2. The method as claimed in claim 1, wherein said act of receiving said one or more keys comprises act of receiving one or more decryption keys are used to for decrypting previously stored content
3. The method as claimed in claim 1, wherein said act of determining comprises act of receiving a notification based on a first criteria.
4. The method as claimed in claim 3, wherein said first criteria comprises act of evaluating if at least one or more previously received keys will be expiring.
5. The method as claimed in claim 3, wherein said first criteria comprises determining if said one or more keys were not received.
6. The method as claimed in claim 1, wherein receiving said non-key data comprises receiving a set of system parameters.
7. The method as claimed in claim 1, wherein receiving said non-key data comprises receiving a set of multi-media data.
8. The method as claimed in claim 1, wherein receiving said non-key data comprises receiving a set of system parameters and a set of multimedia data.
9. The method as claimed in claim 1, further comprising an act of storing said received one or more keys into a database.
10. The method as claimed in claim 1, wherein said act of receiving comprises of receiving said one or more keys from a core network, said core network comprising a digital rights management server and a license key server.
11. An apparatus, operable in a mobile communication system and configured to receive one or more keys, the apparatus comprising:

a processor configured to determine if said one or more keys needs to be requested and requesting delivery of said one or more keys; said processor further configured to receive said one or more keys during a connection scheduled for receiving a non-key data.

12. The apparatus as claimed in claim 11, wherein said one or more keys comprise at one key for decrypting previously stored content.

13. The apparatus as claimed in claim 11, wherein said processor further configured to receive a notification based on a first criteria.

14. The apparatus as claimed in claim 13, wherein said first criteria comprises value of key expiration.

15. The apparatus as claimed in claim 13, wherein said first criteria comprises a value generated, after determining if one or more keys were not received.

16. The apparatus as claimed in claim 11, wherein said non-key data comprises a set of multi-media data.

17. The apparatus as claimed in claim 11, wherein said non-key data comprises a set of system parameters.

18. The apparatus as claimed in claim 11, wherein said non-key data comprises a set of system parameters and a set of multi-media data.

19. The apparatus as claimed in claim 11, wherein said processor further storing said received said one or more keys into a database.

20. The apparatus as claimed in claim 11, wherein said processor further configured to receive said one or more keys, wherein said at least one of said keys comprises a license key.

21. An apparatus for delivering one or more keys, operable in a wireless communication system, the apparatus comprising:

a processor configured to generate said one or more keys to be sent to a mobile device and transmit said generated keys to said mobile device during a connection scheduled for transmitting non-key data.

22. The apparatus as claimed in claim 21, wherein said processor further configured to determine, prior to transmitting, if said mobile device requires at least one key.
23. The apparatus as claimed in claim 21, wherein said processor further configured to send a notification to said mobile device indicating that one or more keys are available for transmission.
24. The apparatus as claimed in claim 21, wherein said processor configured to access a license key server to generate said keys.
25. The apparatus as claimed in claim 21, wherein said processor further configured to access a license key server, a digital rights management server and a distribution center. to generate said keys.
26. The apparatus as claimed in claim 21 said processor further configured to receive a request to transmit keys from said mobile device, prior to generating said keys.
27. The apparatus as claimed in claim 21, said processor further configured to determine a schedule for said connection.
28. The apparatus as claimed in claim 21, said processor further configured to determine if said one or more keys have expired before generating said keys.
29. The apparatus as claimed in claim 21, said processor further configured to attach said keys to a non-key data message containing system parameters.
30. The apparatus as claimed in claim 21, said processor further configured to use key epochs to schedule said connection for transmitting non-key data.
31. A method of delivering one or more keys in a wireless communication system, the method comprising acts of:
- generating said keys to be sent to a mobile device; and
 - transmitting said keys to said mobile device during a connection, scheduled for transmitting non-key data.
32. The method as claimed in claim 31, further comprising an act of:
- determining, prior to transmitting, if required to transmit at least one key.
33. The method as claimed in claim 31, further comprising an act of:

sending a notification indicating that one or more keys are available for transmission.

34. The method as claimed in claim 31, wherein said act of generating comprises an act of accessing a license key server.

35. The method as claimed in claim 31, wherein said act of generating comprises an act of accessing a license key server, a digital rights management server and a distribution center.

36. The method as claimed in claim 31, further comprising an act of receiving a request to transmit keys, prior to generating said keys.

37. The method as claimed in claim 31, further comprising an act of determining a schedule for said connection.

38. The method as claimed in claim 31, further comprising an act of determining if said one or more keys have expired before generating said keys.

39. The method as claimed in claim 31, further comprising an act of attaching said keys to a non-key data message containing system parameters.

40. The method as claimed in claim 31, further comprising an act of using key epochs to schedule said connection for transmitting non-key data.

41. A method of delivering keys from first device to a second device, the method comprising acts of:

generating said keys, at the first device, to be sent to a second device;
and

transmitting said keys from the first device to second device during a connection, scheduled for transmitting non-key data.

42. The method as claimed in claim 41, further comprising acts of:

determining, at the second device, if one or more keys needs to be requested;

requesting the first device to deliver said keys; and

receiving, at the second device, said keys from the first device during a connection scheduled for receiving a non-key data.

43. The method as claimed in claim 41, wherein said first device comprises a server computer.

44. The method as claimed in claim 41, wherein said first device comprises a mobile server computer.

45. The method as claimed in claim 41, wherein said second device comprises a mobile terminal.

46. A machine-readable medium comprising instructions which, when executed by a machine, cause the machine to perform operation including:

determining whether to request one or more keys;

requesting delivery of said keys; and

receiving said keys during a connection scheduled for receiving a non-key data.

47. A machine-readable medium comprising instructions which, when executed by a machine, cause the machine to perform operation including:

generating said keys to be sent to a mobile device; and

transmitting said keys to said mobile device during a connection, scheduled for transmitting non-key data.