US 20090216680A1

(19) **United States**

(12) **Patent Application Publication**

**McCown et al.**

(10) **Pub. No.: US 2009/0216680 A1**

(43) **Pub. Date: Aug. 27, 2009**

(54) **SYSTEMS AND METHODS FOR PERFORMING FILE DISTRIBUTION AND PURCHASE**

(75) Inventors: **Steven H. McCown**, Rigby, ID (US); **Aaron R. Turner**, Idaho Falls, ID (US)

Correspondence Address:
**TraskBritt / Battelle Energy Alliance, LLC**
**PO Box 2550**
**Salt Lake City, UT 84110 (US)**

(73) Assignee: **BATTELLE ENERGY ALLIANCE, LLC**, Idaho Falls, ID (US)

(21) Appl. No.: **12/196,669**

(22) Filed: **Aug. 22, 2008**

**Related U.S. Application Data**

(60) Provisional application No. 61/031,885, filed on Feb. 27, 2008, provisional application No. 61/031,605, filed on Feb. 26, 2008.

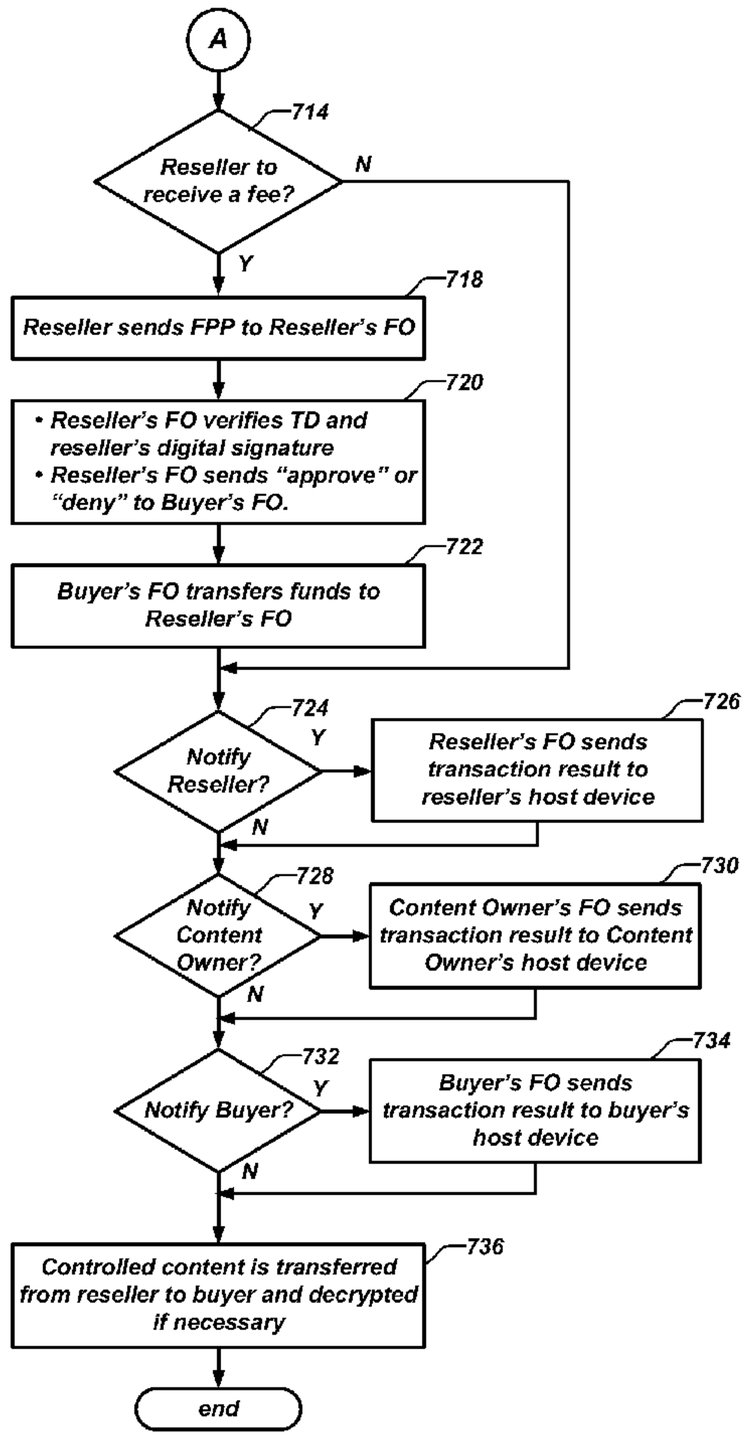
**Publication Classification**

(51) **Int. Cl.**
***G06Q 20/00*** (2006.01)
***H04L 9/32*** (2006.01)

(52) **U.S. Cl.** ..... **705/75**; 705/35; 705/64; 705/44

(57) **ABSTRACT**

A secure computing module (SCM) is configured for connection with a host device. The SCM includes a processor for performing secure processing operations, a host interface for coupling the processor to the host device, and a memory connected to the processor wherein the processor logically isolates at least some of the memory from access by the host device. The SCM generates a secure digital signature for a financial transaction and enables controlled content received through the host device. File distribution is performed from a content provider to a buyer or from a reseller to a buyer. The file distribution includes a financial transaction using secure digital signatures and possibly message encryption. The digital signatures and transaction details are communicated to appropriate financial organizations to authenticate the transaction parties and complete the transaction. The controlled content is transferred to the buyer from either the content provider or the reseller.



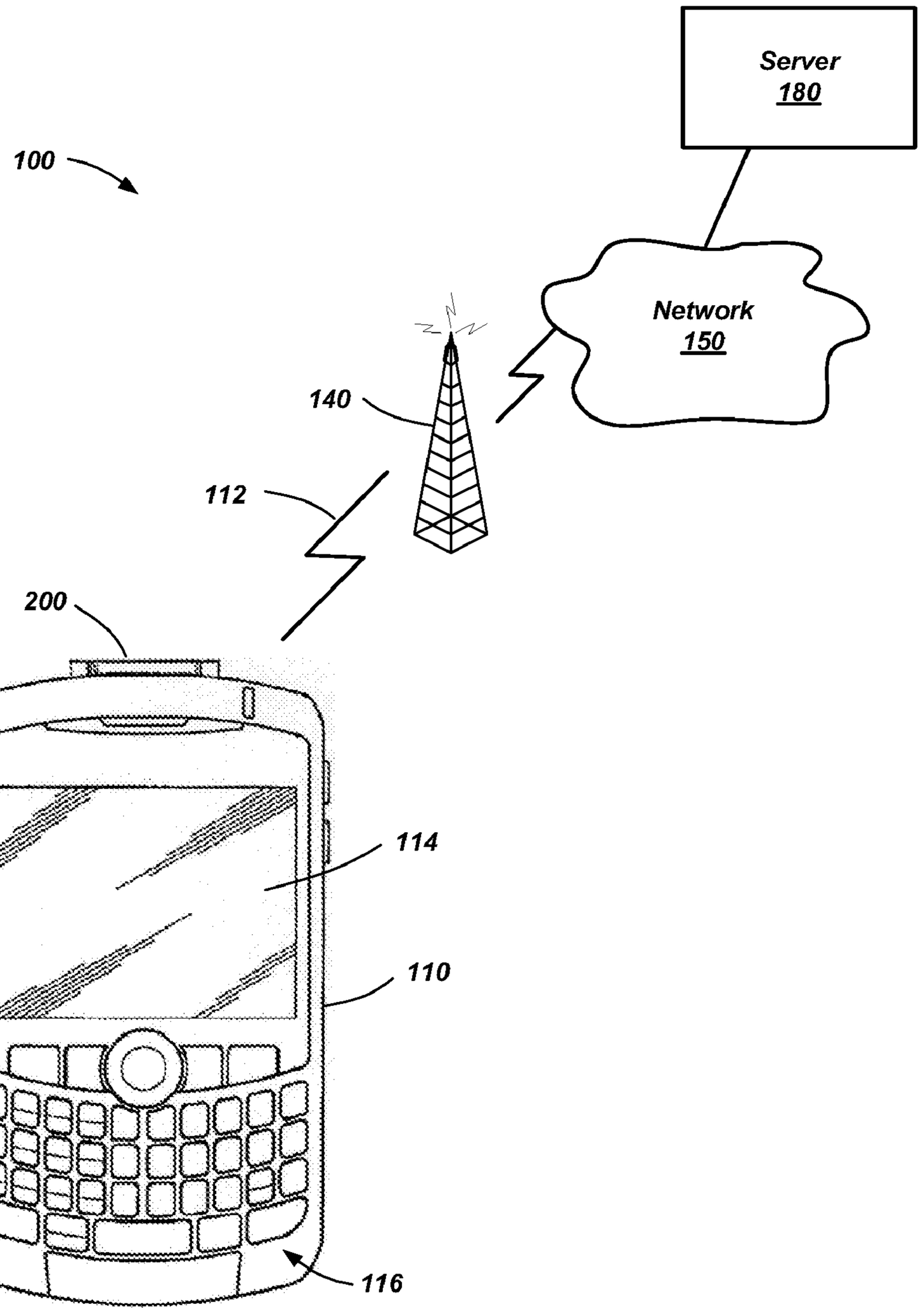



FIG. 1

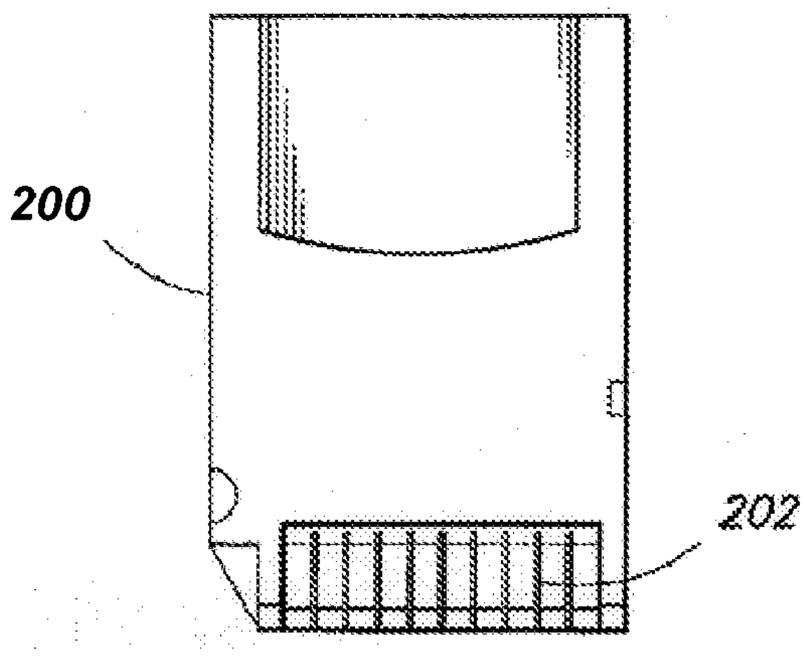



FIG. 2

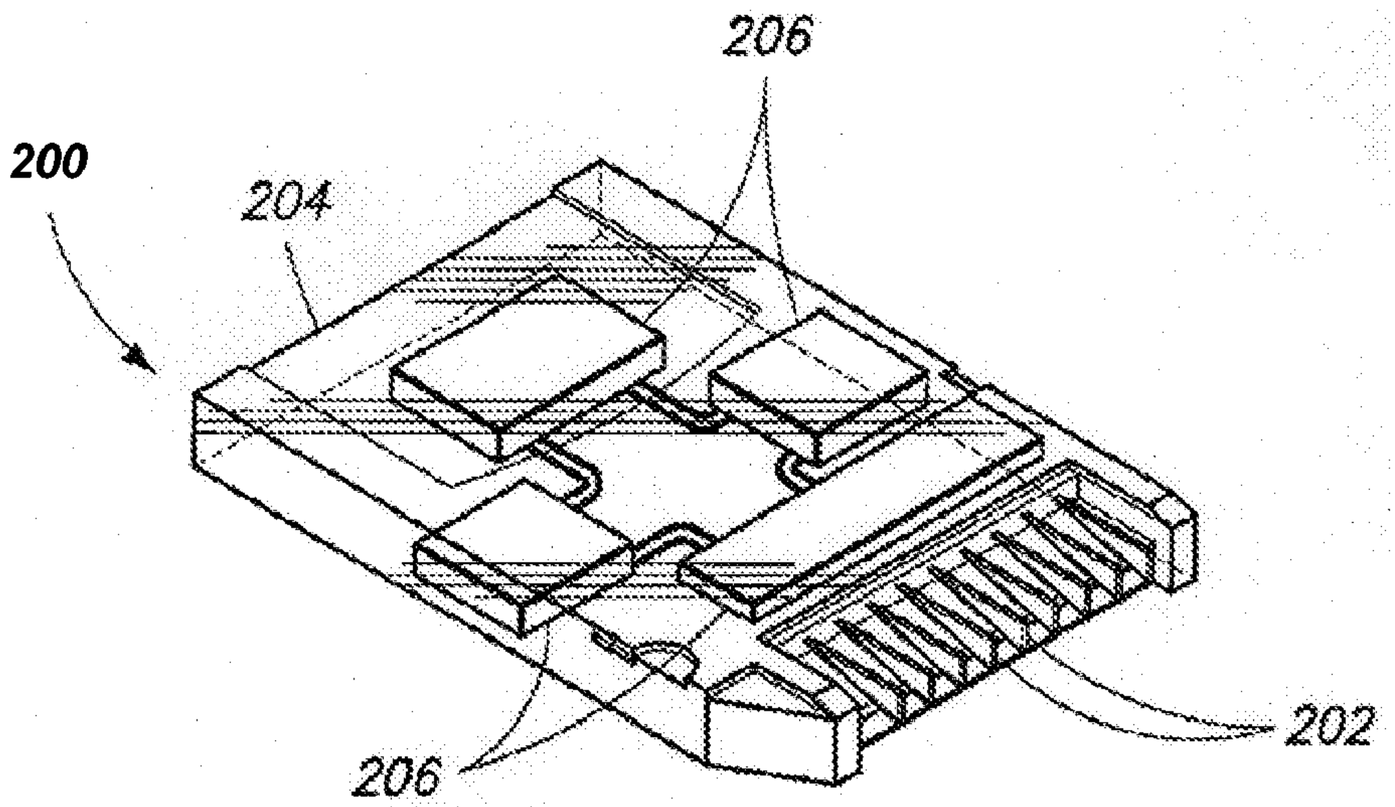



FIG. 2A

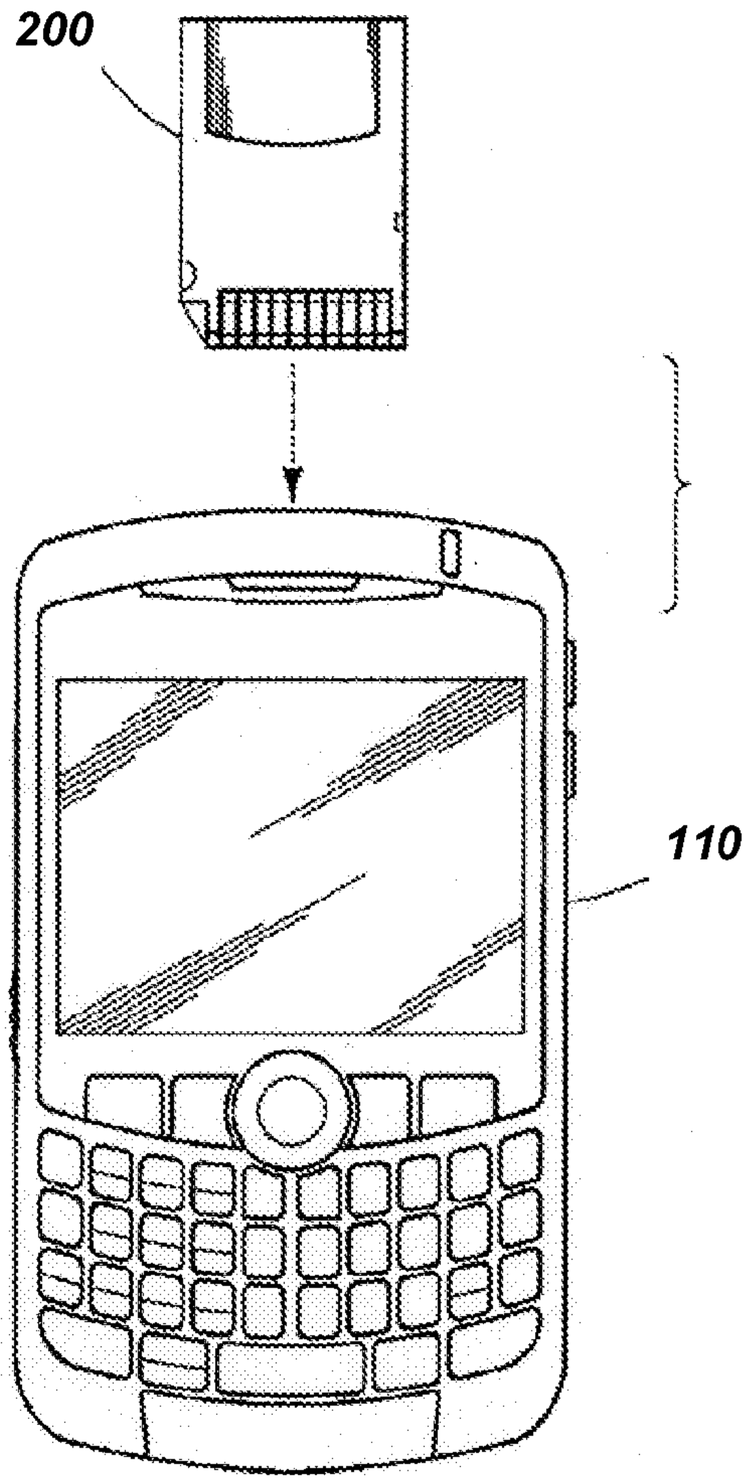



FIG. 3

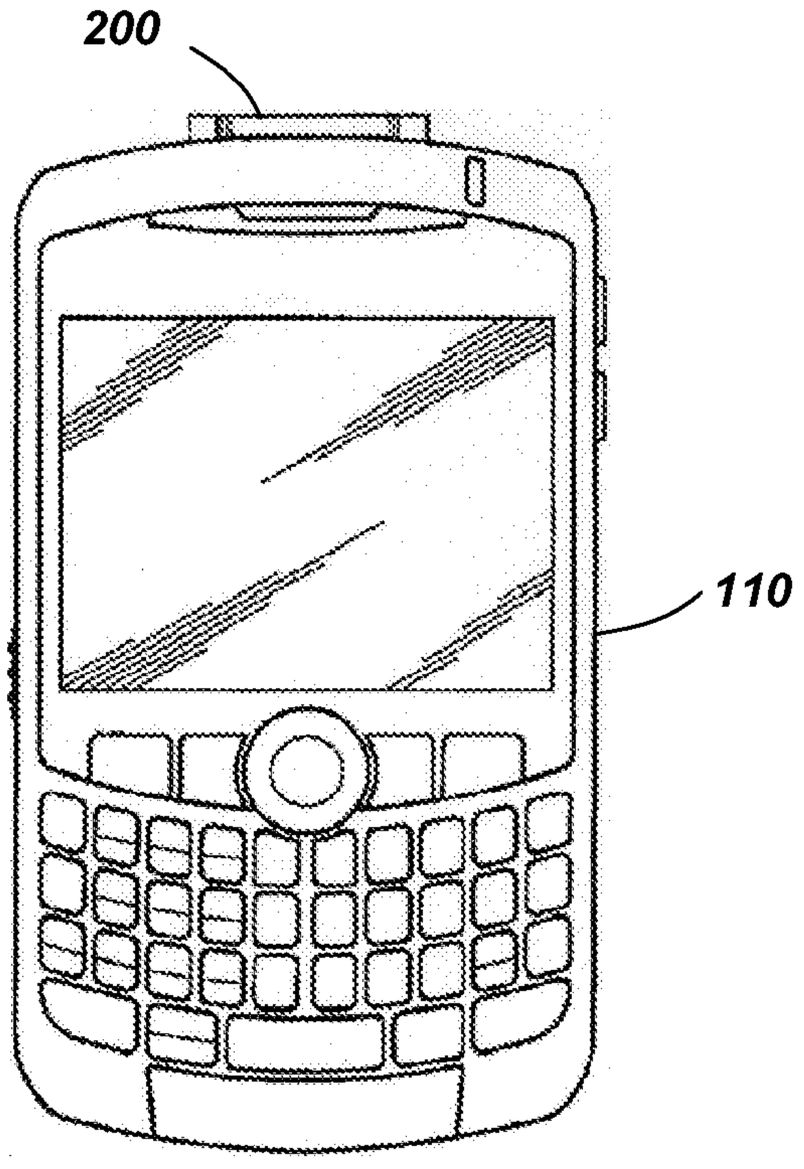



FIG. 3A

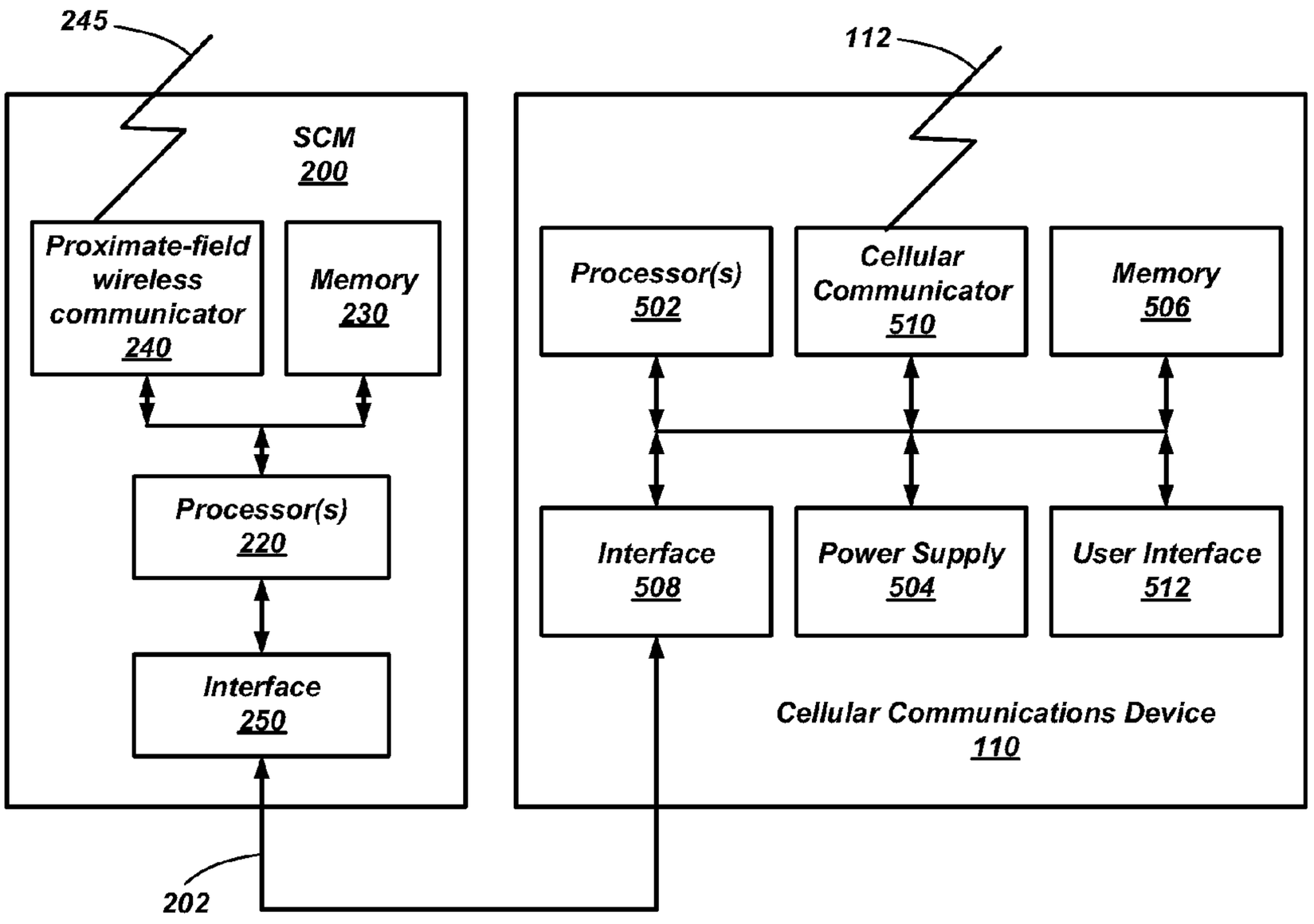

245
112
SCM
200
Proximate-field wireless communicator 240
Memory 230
Processor(s) 220
Interface 250
202
Processor(s) 502
Cellular Communicator 510
Memory 506
Interface 508
Power Supply 504
User Interface 512
Cellular Communications Device 110

FIG. 4

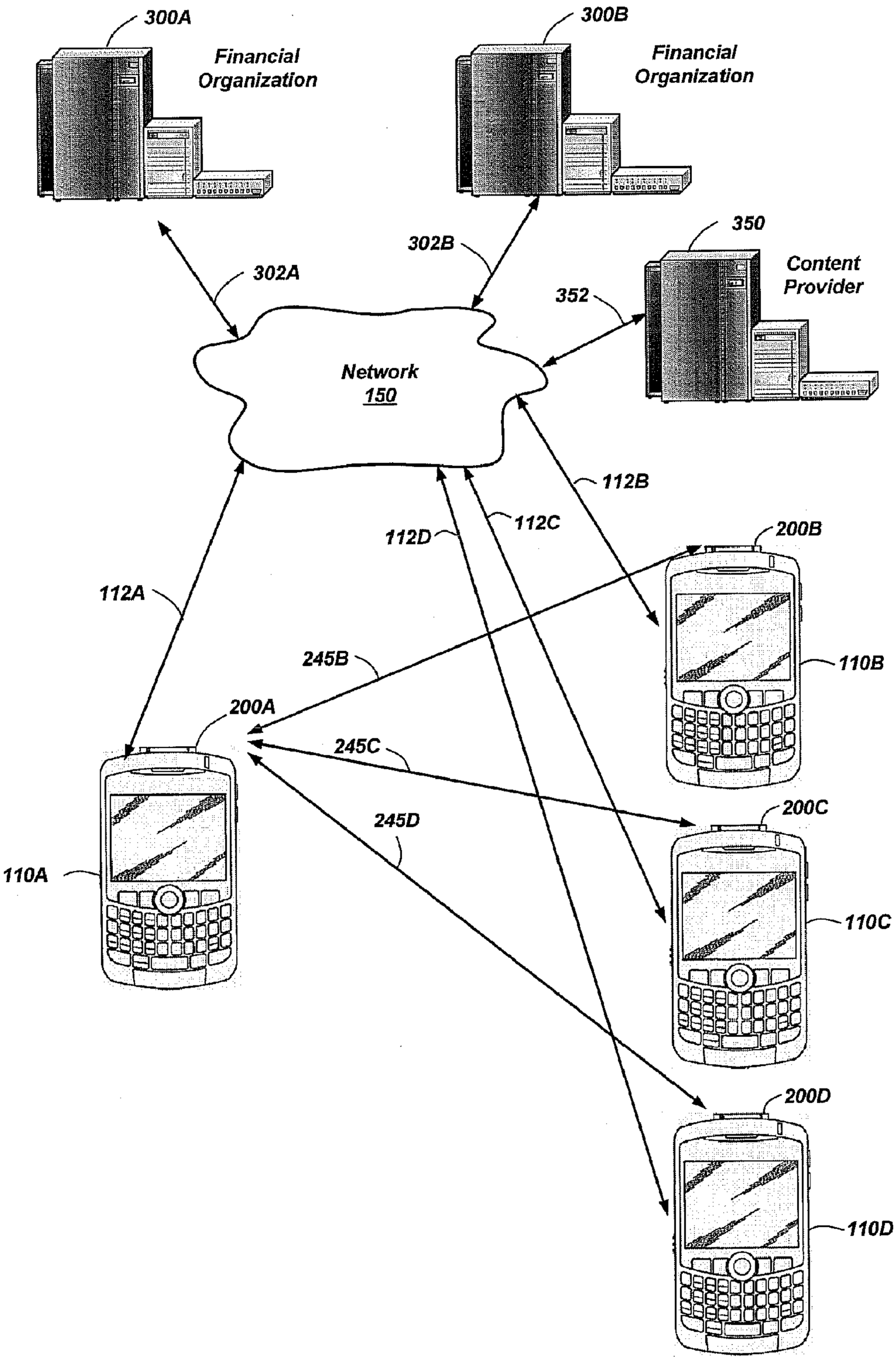

300A
Financial Organization
300B
Financial Organization
350
Content Provider
352
302A
302B
Network
150
112A
112B
112C
112D
200A
200B
200C
200D
110A
110B
110C
110D
245B
245C
245D

FIG. 5

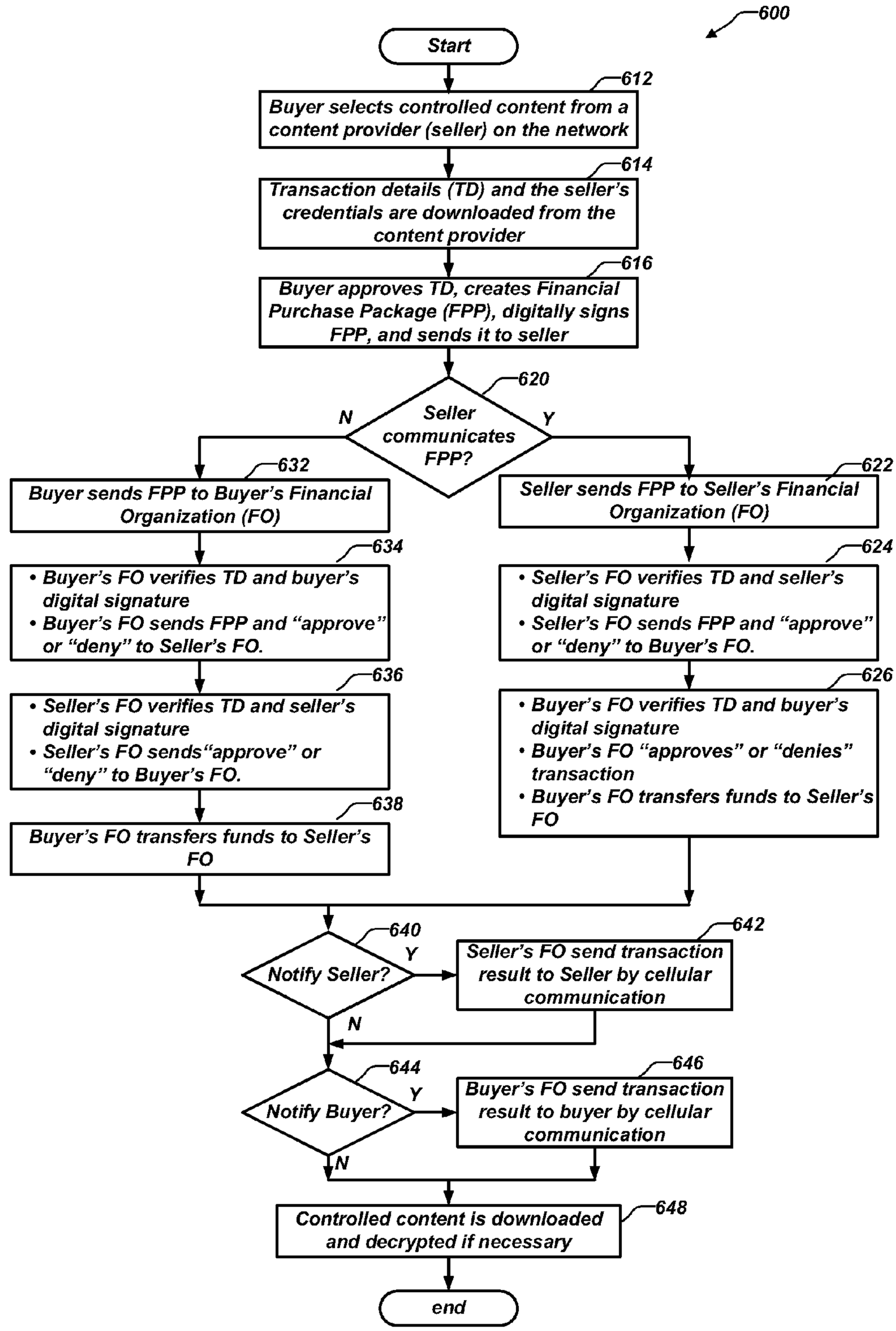

600
Start
612
Buyer selects controlled content from a content provider (seller) on the network
614
Transaction details (TD) and the seller's credentials are downloaded from the content provider
616
Buyer approves TD, creates Financial Purchase Package (FPP), digitally signs FPP, and sends it to seller
620
Seller communicates FPP?
N
Y
632
Buyer sends FPP to Buyer's Financial Organization (FO)
634
• Buyer's FO verifies TD and buyer's digital signature
• Buyer's FO sends FPP and "approve" or "deny" to Seller's FO.
636
• Seller's FO verifies TD and seller's digital signature
• Seller's FO sends"approve" or "deny" to Buyer's FO.
638
Buyer's FO transfers funds to Seller's FO
622
Seller sends FPP to Seller's Financial Organization (FO)
624
• Seller's FO verifies TD and seller's digital signature
• Seller's FO sends FPP and "approve" or "deny" to Buyer's FO.
626
• Buyer's FO verifies TD and buyer's digital signature
• Buyer's FO "approves" or "denies" transaction
• Buyer's FO transfers funds to Seller's FO
640
Notify Seller?
Y
N
642
Seller's FO send transaction result to Seller by cellular communication
644
Notify Buyer?
Y
N
646
Buyer's FO send transaction result to buyer by cellular communication
648
Controlled content is downloaded and decrypted if necessary
end

FIG. 6

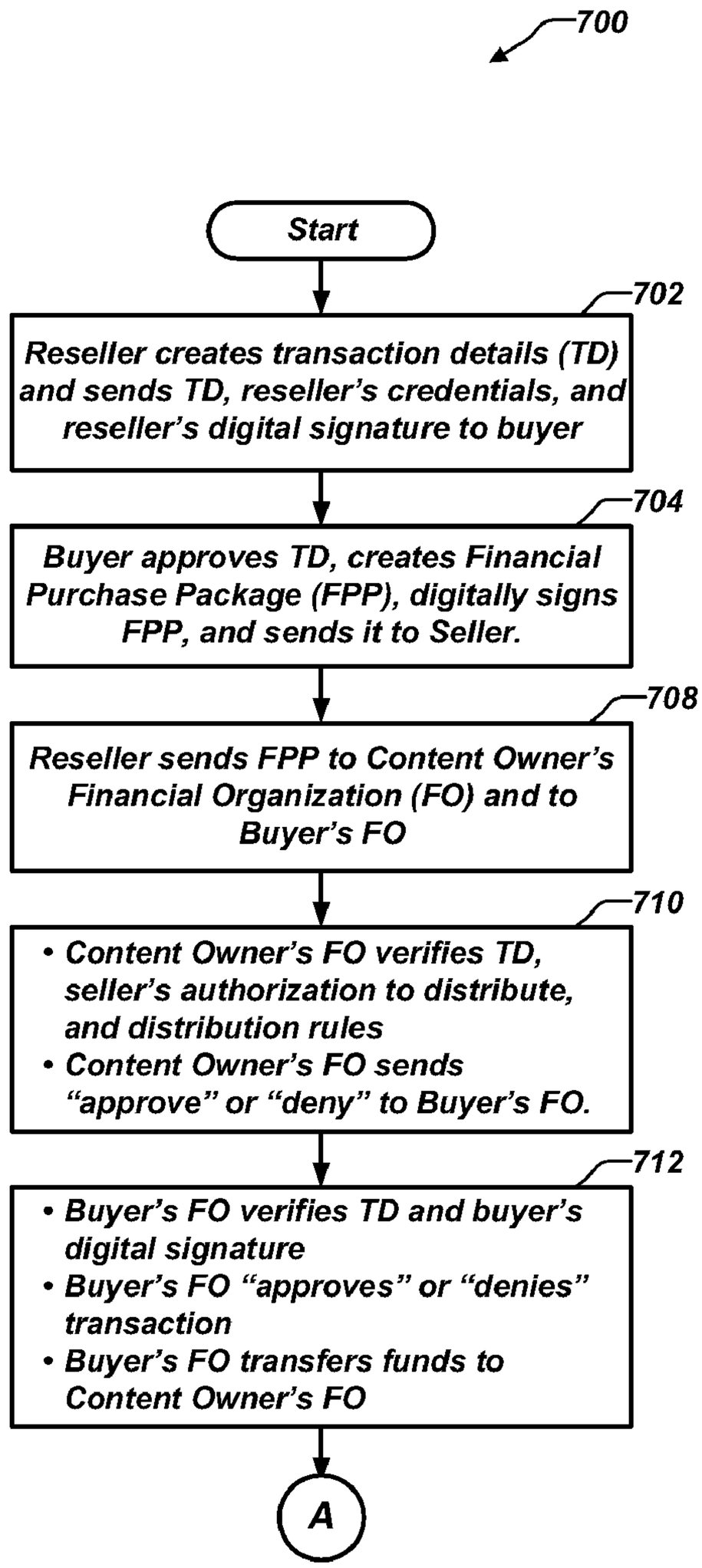

700
Start
702
Reseller creates transaction details (TD) and sends TD, reseller's credentials, and reseller's digital signature to buyer
704
Buyer approves TD, creates Financial Purchase Package (FPP), digitally signs FPP, and sends it to Seller.
708
Reseller sends FPP to Content Owner's Financial Organization (FO) and to Buyer's FO
710
• Content Owner's FO verifies TD, seller's authorization to distribute, and distribution rules
• Content Owner's FO sends "approve" or "deny" to Buyer's FO.
712
• Buyer's FO verifies TD and buyer's digital signature
• Buyer's FO "approves" or "denies" transaction
• Buyer's FO transfers funds to Content Owner's FO
A

FIG. 7A

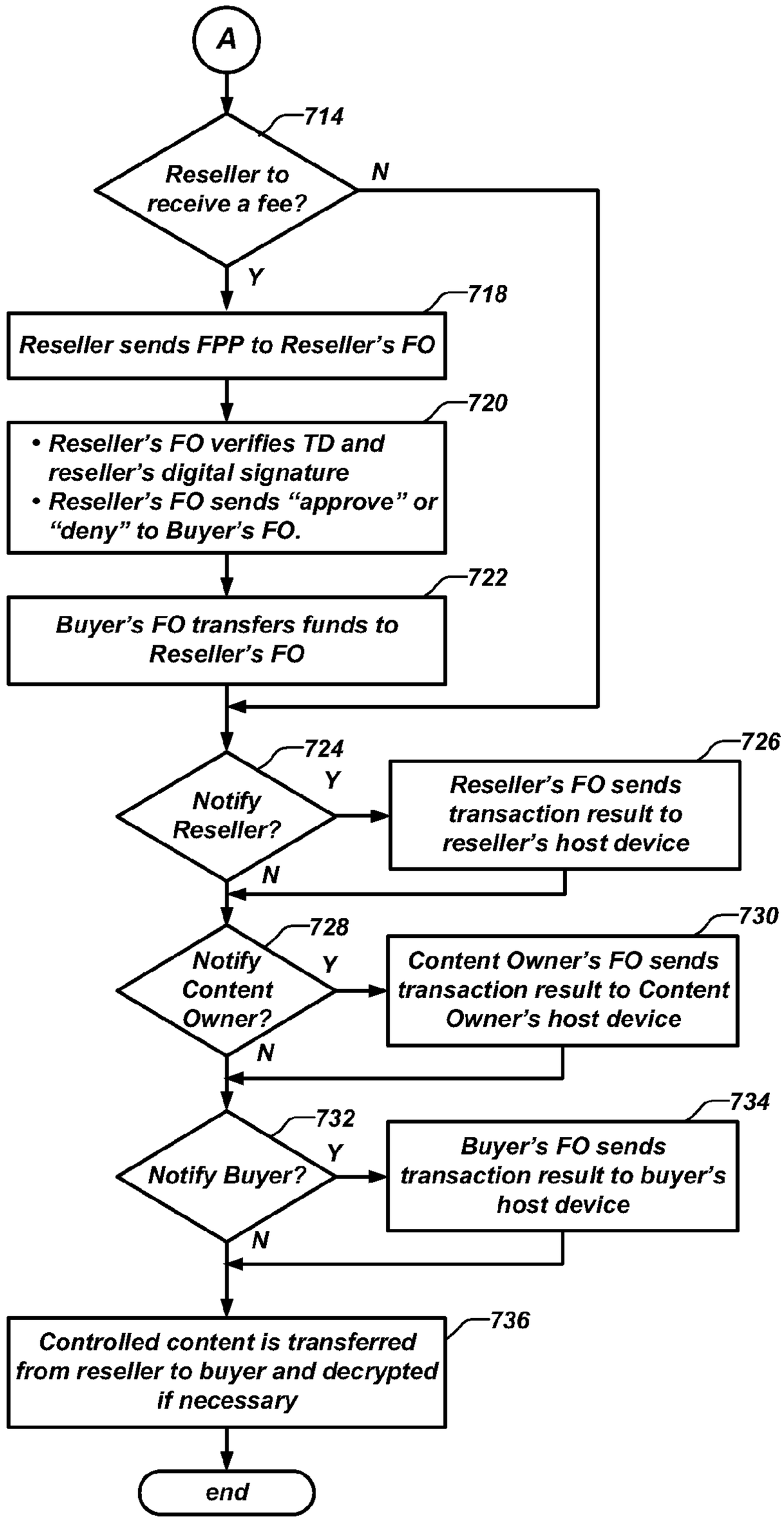

A
714
Reseller to receive a fee?
N
Y
718
Reseller sends FPP to Reseller's FO
720
• Reseller's FO verifies TD and reseller's digital signature
• Reseller's FO sends "approve" or "deny" to Buyer's FO.
722
Buyer's FO transfers funds to Reseller's FO
724
Notify Reseller?
Y
N
726
Reseller's FO sends transaction result to reseller's host device
728
Notify Content Owner?
Y
N
730
Content Owner's FO sends transaction result to Content Owner's host device
732
Notify Buyer?
Y
N
734
Buyer's FO sends transaction result to buyer's host device
736
Controlled content is transferred from reseller to buyer and decrypted if necessary
end

FIG. 7B

# SYSTEMS AND METHODS FOR PERFORMING FILE DISTRIBUTION AND PURCHASE

## RELATED APPLICATIONS

**[0001]** The present Patent Application claims the benefit of U.S. Provisional Patent Application Ser. No. 61/031,885, filed Feb. 27, 2008 and entitled "Phone-to-Phone File Distribution System with Payment," and the benefit of U.S. Provisional Patent Application Ser. No. 61/031,605, filed Feb. 26, 2008 and entitled "Phone-to-Phone Financial Transaction System," each of which application is assigned to the assignee hereof, and the disclosure of each of which application is incorporated herein in its entirety by reference.

**[0002]** This application is also related to U.S. Patent Application (Attorney Docket BA-306) filed on even date herewith and entitled "Systems and Method for Performing Wireless Financial Transactions," assigned to the assignee hereof and the disclosure of which application is incorporated herein in its entirety by reference.

## GOVERNMENT RIGHTS

**[0003]** The United States Government has certain rights in this invention pursuant to Contract No. DE-AC07-05-ID14517, between the United States Department of Energy and Battelle Energy Alliance, LLC.

## TECHNICAL FIELD

**[0004]** Embodiments of the present invention relate generally to wireless communications systems and more specifically to systems and methods of performing financial transactions and file distribution using communication systems.

## BACKGROUND

**[0005]** For many years, cellular telephones were designed primarily to provide wireless voice communications. With new advances in technology, however, additional functionality has been added to cellular telephones, which are sometimes referred to as personal wireless devices. For example, personal wireless devices including the functionality of a cellular phone, personal digital assistant, email client, media player, and a digital camera are now common. Due to the increased capabilities of these devices, many subscribers are using the devices to store or access sensitive information (e.g., financial account information) or to access private networks (e.g., corporate networks).

**[0006]** With respect to financial transactions, security and fraud prevention innovations are vital to market expansion and user acceptance of new forms of wireless transactions. For example, credit card transactions, whether conducted in person or over the Internet, are susceptible to fraud and theft by increasingly sophisticated thieves. Such attacks range from stealing credit card receipts or copying card numbers to attacking web accessible databases in order to acquire massive amounts of credit card account numbers. Fraud from these types of attacks results in billions of dollars in losses each year, both from these initial thefts of funds, as well as the resulting identity theft.

**[0007]** In addition to working toward fraud prevention, credit card companies are continuously seeking novel methods of expanding their customer sets. Many growth activities center on recruiting young people with a perceived need to establish credit, such as those entering the market for the first time, college students with grant money to spend, and people trying to repair bad credit.

**[0008]** With respect to media, peer-to-peer file sharing systems have become the bane of revenue-seeking copyright holders in that traditional file sharing systems provide consumers with copyrighted content without compensating the legal copyright holders for their works.

**[0009]** There is a need for systems and methods to support distribution of controlled content, such as copyrighted works, wherein a secure financial transaction can be performed as part of the distribution. There is also a need to support person-to-person file sharing or distribution of controlled content wherein a secure financial transaction can be performed as part of the sharing or distribution.

## BRIEF SUMMARY OF THE INVENTION

**[0010]** Embodiments of the present invention include systems and methods to support distribution of controlled content, wherein a secure financial transaction can be performed as part of the distribution. Embodiments of the present invention also support person-to-person file sharing or distribution of controlled content wherein a secure financial transaction can be performed as part of the sharing or distribution.

**[0011]** In one embodiment of the present invention, a secure computing module is configured for operable coupling to a host device. The secure computing module includes a processor for performing secure processing operations, a host interface for operably coupling the processor to the host device, and a memory operably coupled to the processor wherein the processor logically isolates at least some of the memory from access by the host device. The secure computing module is configured to generate a secure digital signature for a message including financial transaction details. The secure computing module is also configured to direct the host device to communicate the financial transaction details and the secure digital signature to a financial organization associated with a user of the secure computing module and enable controlled content received through the host device.

**[0012]** In accordance with another embodiment of the present invention, a method of performing file distribution includes selecting controlled content to be received from a content provider acting as a seller. Financial transaction details for the controlled content are sent to a buyer. The method also includes signing the financial transaction details with a buyer's secure digital signature using a buyer's secure computing module and signing the financial transaction details with a seller's secure digital signature using a seller's secure computing module. The financial transaction details, the buyer's secure digital signature, and the seller's secure digital signature comprise a financial transaction package. The method also includes communicating the financial transaction package between the buyer and the seller, communicating the financial transaction package to a seller's financial organization, and communicating the financial transaction package to a buyer's financial organization. The seller's financial organization verifies the seller's secure digital signature and the financial transaction details and sends a seller approval to the buyer's financial organization. The buyer's financial organization verifies the buyer's secure digital signature and the financial transaction details, sends a buyer approval to the seller's financial organization, and performs a fund transfer from the buyer's financial organization to the seller's financial organization. The method also includes

communicating the controlled content from the content provider to the buyer's secure computing module.

**[0013]** In accordance with still another embodiment of the present invention, a method of performing file distribution includes selecting controlled content to be received from a reseller, determining financial transaction details including a transaction amount and a content owner for the controlled content, and sending the financial transaction details for the controlled content to a buyer. The method also includes signing the financial transaction details with a buyer's secure digital signature using a buyer's secure computing module and signing the financial transaction details with a reseller's secure digital signature using a reseller's secure computing module. The financial transaction details, the buyer's secure digital signature, and the reseller's secure digital signature comprise a financial transaction package. The method also includes communicating the financial transaction package between the buyer and the reseller, communicating the financial transaction package to a buyer's financial organization, and communicating the financial transaction package to a content owner's financial organization. The content owner's financial organization verifies the financial transaction details and sends a seller approval to the buyer's financial organization. The buyer's financial organization verifies the buyer's secure digital signature and the financial transaction details, sends a buyer approval to the content owner's financial organization, and performs a fund transfer from the buyer's financial organization to the content owner's financial organization. The method also includes communicating the controlled content from the reseller's secure computing module to the buyer's secure computing module.

## BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

**[0014]** FIG. **1** illustrates a communication system including a host device and a secure computing module;

**[0015]** FIG. **2** illustrates a front view of the secure computing module embodied in a card suitable for insertion into a cellular communication device;

**[0016]** FIG. **2**A illustrates an isometric view of the secure computing module of FIG. **2** with a semi-transparent view to illustrate internal components according to an embodiment of the invention;

**[0017]** FIG. **3** illustrates the secure computing module disconnected from the cellular communication device;

**[0018]** FIG. **3**A illustrates the secure computing module physically and electrically connected to the cellular communication device;

**[0019]** FIG. **4** illustrates a simplified block diagram of the secure computing module in communication with the cellular communication device;

**[0020]** FIG. **5** illustrates a simplified system diagram of a communication system for performing financial transactions and controlled content distribution between individuals;

**[0021]** FIG. **6** is a simplified flow diagram illustrating acts that may be performed during distribution and purchase of controlled content from a content provider; and

**[0022]** FIGS. **7**A and **7**B are simplified flow diagrams illustrating acts that may be performed during distribution and purchase of controlled content between individuals.

## DETAILED DESCRIPTION OF THE INVENTION

**[0023]** In the following detailed description, reference is made to the accompanying drawings which form a part hereof, and in which is shown by way of illustration specific embodiments in which the invention may be practiced. These embodiments are described in sufficient detail to enable those of ordinary skill in the art to practice the invention. It should be understood, however, that the detailed description and the specific examples, while indicating examples of embodiments of the invention, are given by way of illustration only and not by way of limitation. From this disclosure, various substitutions, modifications, additions, rearrangements, or combinations thereof within the scope of the present invention may be made and will become apparent to those skilled in the art.

**[0024]** Embodiments of the present invention include systems and methods to support distribution of controlled content, wherein a secure financial transaction can be performed as part of the distribution. Embodiments of the present invention also support person-to-person file sharing or distribution of controlled content wherein a secure financial transaction can be performed as part of the sharing or distribution. In addition, embodiments of the present invention provide systems and methods that collect and preserve market accepted financial revenues (e.g., royalties, payments, etc.) for legal holders of controlled content. Furthermore, embodiments of the present invention provide systems and methods to refine and validate person-to-person marketing, sales, and distribution mechanisms in order to incentivize users to legally share and disseminate controlled content using person-to-person discovery and distribution methods.

**[0025]** The systems and methods include controlled content distribution and secure financial transactions by augmenting Personal Electronic Devices (PEDs) with software and a Secure Computing Module (SCM) for executing the software. The SCM may be processing hardware that is either embeddable or embedded in the PED.

**[0026]** As used herein, a PED may be any mobile computing device used by a user and capable of communication using a cellular wireless communication channel. A PED may also be referred to herein as a host device, a cellular communication device, or a wireless communication device. Examples of PEDs include cell phones, smartphones, Blackberry® smart phones, pagers, Personal Digital Assistants, music players (e.g., MP3 players and IPods), handheld computing platforms, wrist-worn computing system, or other mobile computing systems (e.g., laptops). In addition, the host device may be a desktop computer, server, or other device such as, for example, satellite TV receivers, Digital Versatile Disc (DVD) players, and Video Cassette Recorders (VCRs) equipped with a secure computing module. While most of the description herein concentrates on PEDs as wireless communication devices, those of ordinary skill in the art will recognize that any suitable host device may be configured to operate with a secure computing module to practice embodiments of the present invention.

**[0027]** As used herein, "controlled content" refers to any copyrighted material or any material that can be considered for copyright. Such examples include, but are not limited to, the following: music, videos, eBooks, software, documents, maps, databases, store discount coupons, merchant loyalty material, pictures, or other digital content. Furthermore, controlled content includes access authorization tokens. As non-limiting examples, access authorization tokens may include electronic tickets (i.e., e-tickets) for admittance to movies, concerts, sporting events, and the like.

**[0028]** As used herein, a "content owner" is an entity or individual that may, according to national law, international law, or combination thereof, own at least some of the rights to controlled content that they have rights to control access to, created themselves, or legally purchased.

**[0029]** As used herein, a "content provider" is the content owner or agent of the content owner authorized to provide controlled content owned by the content owner.

**[0030]** As used herein, "distribution rules" are rules defining the rights and methods of distribution. Such rules may limit distribution to specific groups, time periods, numbers, etc.

**[0031]** As used herein an "original buyer" is a buyer who purchases controlled content directly from the content owner or an agent of the content owner.

**[0032]** As used herein, a "reseller" is a buyer who is authorized to resell controlled content according the distribution rules specified by the content owner.

**[0033]** FIG. **1** illustrates a communication system **100** including a host device **110**, a server **180**, a network **150**, a wireless communications base station **140**, and a secure computing module **200**.

**[0034]** In some embodiments, the host device **110** may be a cellular communication device **110**. The cellular communication device **110** may communicate with the base station **140** using a wireless channel **112**, which may be a cellular wireless channel. The cellular communication device **110** may be a wireless communication device, such as a smart phone, Blackberry® smart phone, laptop computer, or other suitable device configured to communicate with a terrestrial cellular base station **140**. The base station **140** may communicate with the network **150**. The network **150** may be a communications network such as the Internet, the public switched telephone network, or any other suitable arrangement for implementing communications.

**[0035]** The cellular communication device **110** may include a display for communicating information to a user and a keypad for the user to communicate information to the cellular communication device **110**.

**[0036]** The secure computing module **200** may be physically connected to the cellular communication device **110**. As a non-limiting example, the secure computing module **200** may be configured as a card suitable for insertion into the host device **110**. Although physically connected to the host device **110**, the secure computing module **200** may execute software independently and/or isolated from the host device **110**.

**[0037]** FIG. **2** illustrates a front view of the secure computing module **200** embodied in a card suitable for insertion into the cellular communication device **110**. FIG. **2**A illustrates an isometric view of the secure computing module **200** of FIG. **2** with a semi-transparent view to illustrate internal components according to an embodiment of the invention. The secure computing module **200** may have physical characteristics similar to a Secure Digital (SD) memory card. For example, the secure computing module **200** may include a housing **204** having dimensions substantially similar to an SD memory card. Furthermore, the secure computing module **200** may include a host interface **202** configured to be physically and electrically connected to the cellular communication device **110**. As non-limiting examples, the host interface **202** may be configured as an SD Input/Output (SDIO) interface, a Secure Digital High Capacity (SDHC) interface, or other interface suitable for plugging into an expansion suitable for plugging into an SD slot of the cellular communication device **110**. As illustrated in FIG. **2**A, the secure computing module **200** may include the housing **204**, circuitry **206**, and the host interface **202**.

**[0038]** The housing **204** encompasses the circuitry **206** and may allow a user to handle the secure computing module **200** without damaging the circuitry **206** by surrounding the circuitry **206**, so that circuitry **206** is not physically exposed to the user.

**[0039]** As shown in FIGS. **2** and **2**A, some embodiments may be configured such that the housing **204** including the secure computing module **200** is different from and removable from the host device **110**. In other embodiments, the secure computing module **200** may not include a housing and may be embedded in with the cellular communication device **110**. In any embodiment, the secure computing module **200** is configured to maintain at least a logical isolation from the cellular communication device **110**, as is explained more fully below.

**[0040]** The circuitry **206** may comprise one or more integrated circuits and may comprise one or more circuit boards. The circuitry **206** may be configured to perform the functionality of the secure computing module **200**.

**[0041]** Of course, the secure computing module **200** may be configured with a form factor other than an SD form factor. For example, the secure computing module **200** may have the physical characteristics (e.g., dimensions) of a TransFlash, miniSD, microSD, memory stick, compact flash, Multi Media Card (MMC), reduced size MMC, MMC micro, smart media, smart card, mini smart card, xD memory card, or other suitable form factor compatible with the cellular communication device **110**.

**[0042]** As another non-limiting example, the host interface **202** may be a serial bus, such as, for example, a Universal Serial Bus (USB) interface or "firewire" interface suitable for compatible connections to the cellular communication device **110**. Other physical configurations and host interface formats that enable the secure computing module **200** to be operably coupled to the host device **110** are also possible.

**[0043]** Although the physical characteristics (e.g., dimensions) of the secure computing module **200** and the host interface **202** may be similar to one of the above-mentioned memory card formats, the secure computing module **200** may perform functionality beyond that performed by a memory card as is discussed more fully below.

**[0044]** FIG. **3** illustrates the secure computing module **200** disconnected from the cellular communication device **110**. In other words, a user of the secure computing module **200** may connect the secure computing module **200** to the cellular communication device **110** and may later disconnect the secure computing module **200** from the cellular communication device **110**. In general, with removable card formats, the user may disconnect the secure computing module **200** from the cellular communication device **110** by hand without tools and without damaging the secure computing module **200**.

**[0045]** A user may connect the secure computing module **200** to the cellular communication device **110** by inserting the secure computing module **200** into a receptacle of the cellular communication device **110** thereby physically and electrically connecting the secure computing module **200** to the cellular communication device **110**. In some embodiments, the secure computing module **200** may be inserted into a slot formed within the housing of the cellular communication device **110**.

**[0046]** With removable card formats, the secure computing module **200** may be used in more than one the cellular communication device **110** at different moments in time. For example, a user of the secure computing module **200** may use the secure computing module **200** in the cellular communication device **110** and may then later use the secure computing module **200** in a different cellular communication device **110**.

**[0047]** FIG. **3**A illustrates the secure computing module **200** physically and electrically connected to the cellular communication device **110**. In some embodiments, the secure computing module **200** may operate by using power supplied by the cellular communication device **110** and may receive power from the cellular communication device **110** via the host interface **202** (FIG. **2**A). Thus, the secure computing module **200** might not be configured to operate when disconnected from the cellular communication device **110** other than to store data in non-volatile memory. In other embodiments, the secure computing module **200** may include its own internal power source.

**[0048]** In some embodiments, the secure computing module **200** may communicate directly with the base station **140**, network **150**, or server **180**. In other embodiments, the secure computing module **200** may communicate with the base station **140**, network **150**, and server **180** through the host interface **202** and the cellular communication device **110**. Accordingly, the cellular communication device **110** may receive information from the secure computing module **200** and forward the information to the network **150**. Conversely, the cellular communication device **110** may receive information from the network **150** and forward that information on to the secure computing module **200**.

**[0049]** FIG. **4** illustrates a simplified block diagram of the secure computing module **200** in communication with the cellular communication device **110**. The cellular communication device **110** may include an interface block **508** for communicating with the host interface **202**, one or more processors **502**, a power supply **504**, memory **506**, a cellular communicator **510**, and a user interface **512**.

**[0050]** The secure computing module **200** may include one or more processors **220**, memory **230**, a proximate-field wireless communicator **240**, and an interface block **250** for communicating on the host interface **202**.

**[0051]** The processor **220** may be implemented as one or more of a general purpose microprocessor, a special purpose microprocessor, a microcontroller, other suitable hardware, such as, for example, an Application Specific Integrated Circuit (ASIC) or Field Programmable Gate Array (FPGA), or combinations thereof. These examples for the processor **220** are for illustration and other configurations are possible. The interface block **250** is configured to communicate on the host interface **202**, as described earlier.

**[0052]** The secure computing module **200** is configured for executing software programs containing computing instructions. The one or more processors **220** may be configured for executing a wide variety of operating systems and applications including the computing instructions for carrying out embodiments of the present invention.

**[0053]** The memory **230** may be used to hold computing instructions, data, and other information for performing a wide variety of tasks including performing embodiments of the present invention. The memory **230** may be embodied in a number of different forms using electronic, magnetic, optical, electromagnetic, or other techniques for storing information. By way of example, and not limitation, the memory **230** may include Synchronous Random Access Memory (SRAM), Dynamic RAM (DRAM), Read-Only Memory (ROM), Flash memory, and the like.

**[0054]** The proximate-field wireless communicator **240** is configured for wireless communication across the proximate-field wireless communication channel **245** to another suitably equipped proximate-field wireless communicator. In some embodiments, the other suitably equipped proximate-field wireless communicator may be configured as part of another secure computing module **200**, another secure computing module **200** configured in another cellular communication device **110**, or a point-of-sale terminal configured for wireless communication.

**[0055]** The secure computing module **200** may use functionality provided by the cellular communication device **110**. For example, the cellular communication device **110** may include a user interface **512** comprising a display **114** (FIG. **1**) and a keypad **116** (FIG. **1**). Since the secure computing module **200** might not have a user interface, the secure computing module **200** may provide user interaction data and instruct the cellular communication device **110** to display the information on the display **114**. Similarly, the secure computing module **200** may request that the cellular communication device **110** provide the secure computing module **200** with user interaction data entered by a user on the keypad **116**.

**[0056]** In some embodiments, the power supply **504** may provide power to the secure computing module **200**. In other embodiments, the secure computing module **200** may include its own power supply (not shown).

**[0057]** The proximate-field wireless communication channel **245** may be any wireless frequency and protocol configured for somewhat localized communication. Some non-limiting examples of suitable protocols and frequencies are: suitable Radio Frequencies, 802.1 a/b/gin type wireless connections, infrared frequencies, Bluetooth® Radio Frequency Identification (RFID), WiFi, WiMax, or other suitable communication definitions. As non-limiting examples, distances of less than an inch to a few inches for RFID communication up to about **100** feet for Bluetooth® communication are considered suitable proximate-field ranges.

**[0058]** FIG. **5** illustrates a simplified system diagram of a communication system for performing financial transactions and controlled content distribution between individuals. The communication system may include two or more cellular communication devices equipped with a secure computing module. The communication system may include a first host device **110**A including a first secure computing module **200**A and additional host devices, such as, for example, a second host device **110**B including a second secure computing module **200**B, a third host device **110**C including a third secure computing module **110**C, and a fourth host device **110**D including a fourth secure computing module **200**D.

**[0059]** For ease of description, the first host device **110**A and the first secure computing module **200**A may be referred to differently depending on the operations performed and the context of the operations. For example, in the context of an original buyer purchasing controlled content from a content provider, the first host device **110**A and the first secure computing module **200**A may be referred to as a buyer's host device **110**A and a buyer's secure computing module **200**A, respectively. As another example, in the context of a reseller providing controlled content to another buyer, the first host device **110**A and the first secure computing module **200**A

may be referred to as a reseller's host device **110**A and a reseller's secure computing module **200**A, respectively.

**[0060]** A secure computing module (designated generically as **200**) may communicate with another secure computing module **200** using the proximate-field wireless communication channels (for example **245**B, **245**C, and **245**D). Any of the host devices (designated generically as **110**) may communicate with the network, which may be via wired or wireless communication. In the case of cellular communication devices, the communication may occur over cellular communication channels **112**A, **112**B, **112**C, and **112**D.

**[0061]** A first financial organization **300**A may be operably coupled to the network over communication channel **302**A. Similarly, a second financial organization **300**B may be operably coupled to the network over communication channel **302**B and a content provider **350** may be operably coupled to the network over communication channel **352**. As non-limiting examples, the communication channels **302**A, **302**B, and **352** may be through the Internet, cellular communication, phone networks, or other suitable connection.

**[0062]** Depending on the context, the first financial organization **300**A may be referred to as a buyer's financial organization or a reseller's financial organization, as will be apparent in the description below. Similarly, depending on the context, the second financial organization **300**B may be referred to as a content provider's financial organization, a seller's financial organization, or a buyer's financial organization, as will be apparent in the description below.

**[0063]** In some embodiments, the seller's financial organization and the buyer's financial organization may be the same entity. Furthermore, in performing financial transactions, the sellers financial organization and the buyer's financial organization may be considered substantially similar to the server **180** of FIG. **1**. In addition, financial organizations may be referred to generically herein with the designator **300**.

**[0064]** FIG. **5** does not illustrate, but it would be understood by a person of ordinary skill in the art that when the host device (**110**A-**110**D) is a cellular device, the cellular communication channels (**112**A-**112**D) generally communicate with the network **150** via a base station **140** as illustrated in FIG. **1**.

**[0065]** Software processes illustrated herein are intended to illustrate representative processes that may be performed by one or more computing systems in carrying out embodiments of the present invention. Unless specified otherwise, the order in which the processes are described is not to be construed as a limitation. Furthermore, the processes may be implemented in any suitable hardware, software, firmware, or combinations thereof. By way of example, software processes may be stored in the memory **230** for execution, and executed by the one or more processors **220**.

**[0066]** When executed as firmware or software, the instructions for performing the processes may be stored or transferred on a computer-readable medium. A computer-readable medium includes, but is not limited to, magnetic and optical storage devices such as disk drives, magnetic tape, CDs (compact disks), DVDs (digital versatile discs or digital video discs), and semiconductor devices such as RAM, DRAM, ROM, EPROM, and Flash memory.

**[0067]** In addition, the firmware or software may be communicated via a network. As non-limiting examples, programming may be provided via appropriate media including, for example, embodied within articles of manufacture, embodied within a data signal (e.g., modulated carrier wave, data packets, digital representations, etc.) communicated via an appropriate transmission medium, such as a communication network (e.g., the Internet and/or a private network), wired electrical connection, optical connection and/or electromagnetic energy, for example, via a communications interface, or provided using other appropriate communication structure or medium. Exemplary programming including processor-usable software may be communicated as a data signal embodied in a carrier wave in but one example.

**[0068]** In addition, it is noted that the examples may be described as a process that is depicted as a flowchart, a flow diagram, a structure diagram, or a block diagram. Although a flowchart may describe the operations as a sequential process, many of the operations can be performed in parallel or concurrently. In addition, the order of the operations may be re-arranged. A process is terminated when its operations are completed. A process may correspond to a method, a function, a procedure, a subroutine, a subprogram, etc. When a process corresponds to a function, its termination corresponds to a return of the function to the calling function or the main function.

**[0069]** In operation for performing controlled content distribution and financial transactions and referring to FIGS. **4** and **5**, the host device **110** is used to interface with a user to solicit input and display pertinent information under direction from the secure computing module **200**. Software executing on the secure computing module **200** manages the financial transaction process and the controlled content transfers. This software may be in the form of a standalone application, device embedded software, or may operate within a web browser native to the device all of which can connect to the secure computing module **200**. Additionally, the software may include an Application Program Interface (API), a Software Development Kit (SDK) or other suitable software interfaces and tools for generating and managing the software of the secure computing module **200**.

**[0070]** The secure computing module **200** provides secure information storage for variables required for the financial transaction processes, such as public and private keys for signing and encryption, secret hashing keys, counter variable (s), etc. The secure computing module **200** also provides secure memory **230** and a secure processing environment for stored procedures such as hashing algorithms, encryption algorithms, counter incrementing, and other suitable secure processes.

**[0071]** Thus, the secure computing module **200** and secure memory **230** provide a logically isolated environment for computing hashes and encrypting information that is from external sources such as the host device **110** and other secure computing modules **200**.

**[0072]** Executing the software in isolation on the secure computing module **200** rather than on the host device **110** may protect data generated by the software against unauthorized access, for example, by malicious software installed on the host device **110**, by a user of the host device **110**, or by a device having connectivity to the host device **110** through the network **150** and the base station **140**.

**[0073]** In addition, the secure computing module **200** may be used to validate all input from external sources. As a non-limiting example, the secure computing module **200** may verify a signed transaction using the public signing key of the other party to the financial transaction.

**[0074]** When using encryption or hashing algorithms, the particular encryption scheme or encryption key may be known by the secure computing module **200** but not by the

host device **110**. As a result, the secure computing module **200** may disregard information received from the host device **110** that is not encrypted according to the particular encryption scheme or with the particular encryption key. Disregarding information not encrypted appropriately may prevent the host device **110** from interacting with the secure computing module **200** other than to relay user interface information between a user interface of the host device **110**, the network **150**, or the server **180**.

**[0075]** The processor **220** may logically isolate some or all of the memory **230** from access by the processor **502** in the host device **110**. In other words, the host interface **202** might not be able to communicate with the memory **230** except via permission and control of the processor **220**, thereby preventing direct communication between the host interface **202** (or a device connected to the host interface **202** such as the host device **110**) and the memory **230**. In addition, the memory **230** may be physically isolated from prying access.

**[0076]** The secure computing module **200** may be pre-installed with protected information, such as, for example, financial transaction software and protected data (e.g., keys) from the vendor, manufacturer, or a combination thereof. In addition, the protected information may be updated on an already deployed system.

**[0077]** In deploying protected information, the protected information may be communicated to the secure computing module **200** using an encrypted information transfer process, wherein the information may include data, software, or a combination thereof. Upon valid decryption and verification of authenticity (i.e., that the software and data originated at the financial organization), the data and algorithms (i.e., software procedures) may be updated within the secure computing module **200**.

**[0078]** The secure computing module **200** may request that the host device **110** retrieve the software from the server **180** (e.g., a web server, Supervisory Control and Data Acquisition (SCADA) server, corporate network server, financial organization **300**A or **300**B, or other server). As a non-limiting example of a buyer update, the buyer's host device **110**A may retrieve the software from the buyer's financial organization **300**A via cellular communication channel **112**A then provide the software to the buyer's secure computing module **200**A. The secure computing module **200**A may decrypt the software if necessary, then install and execute the software. When encrypted, the host device **110** is unable to decrypt the encrypted software. Accordingly, upon retrieving encrypted software, the host device **110** simply forwards the encrypted software to the secure computing module **200** without decrypting the software.

**[0079]** The secure computing module **200** may additionally or alternatively request that the host device **110** send software or other information to the server **180** (FIG. **1**). For example, the secure computing module **200** may encrypt financial information (e.g., an account number, a personal identification number, etc.), provide the encrypted information to the host device **110**, and instruct the host device **110** to send the encrypted information to the server **180**. Since the information, in this example, is encrypted, the host device **110** may be unable to decrypt the financial information.

**[0080]** Driver software may be installed on the host device **110** to assist the host device **110** in communicating with the secure computing module **200** and performing portions of financial transactions. As a non-limiting example, the driver software may enable communication on the host interface **202** according to an established smart card interaction standard (e.g., PC/SC). As another non-limiting example, the driver software may perform information presentation on the display **114** (FIG. **1**) and information retrieval from the keypad **116** (FIG. **1**) and communicate the user interaction information to or from the secure computing module **200**.

**[0081]** The secure computing module **200** includes cryptographic algorithms for creating and decoding secure digital signatures. In addition, the secure computing module **200** may include cryptographic algorithms for encrypting and decrypting information. Thus, the secure portions of the memory **230** may include information such as the cryptographic algorithms, encryption keys, decryption keys, signing keys, counters, and other suitable cryptographic information.

**[0082]** Embodiments of the present invention include a process for creating a secure digital signature for a financial purchase package. The secure digital signature may be prepared by creating a cryptographically secure hash of financial transaction details in combination with a secret key. Any cryptographically secure hashing function in combination with a secret key may be used to fulfill the secure signing function. Furthermore, hashing algorithms and secret keys may be periodically updated by a financial organization associated with the user of the secure computing module **200**.

**[0083]** The secret key is known only to the user's secure computing module **200** and the user's financial organization **300**. However, the secure computing module **200** may be configured to handle multiple financial accounts. Thus, the secure computing module **200** may have a secret key for each account and the secret key for each account would be known by the financial organization servicing that account.

**[0084]** The financial transaction details may include a variety of information, such as, for example:

**[0085]** description of the item(s) being sold;

**[0086]** price of the item(s) (i.e., transaction amount);

**[0087]** the time of transaction;

**[0088]** the date of transaction;

**[0089]** the location of the transaction (e.g., via GPS coordinates—if available);

**[0090]** the buyer's credential and financial organization routing numbers; and

**[0091]** the seller's credential and financial organization routing numbers.

**[0092]** The credentials of the buyer or the seller may include information such as, for example, account information such as account number and financial organization identification, a public key, and other suitable information. The credentials are used to uniquely identify an individual to the financial organization. Anonymity may be maintained through this process allowing a buyer or seller to withhold their identity from the other party. However, each party must be uniquely identified to the financial organizations in order for funds to transfer. If anonymity is not desired, the credentials may also include the user's name.

**[0093]** Embodiments of the present invention include a Financial Purchase Package (FPP) which, when completed, includes the financial transaction details, a buyer's secure digital signature, and a seller's secure digital signature.

**[0094]** The secure digital signature for both the buyer and the seller may be created with a secure hashing function using a secret key. Secure hashing functions come in many forms and are occasionally standardized by government bodies such as the National Institute of Standards and Technology

(NIST). As new cryptographically secure hashing functions using secret keys are standardized, they may be incorporated into the secure computing module **200**.

**[0095]** A non-limiting example of a secure hash using a secret key is described in Federal Information Processing Standard (FIPS) Publication **198**, which is incorporated by reference herein. In general terms, the hashing function may be represented by the following equation:

$$HMAC_K(m)=h((K\oplus opad)\|h((K\oplus ipad)\|m))$$

**[0096]** In this equation, h is a cryptographic hash function, K is a secret key padded with extra zeros to the block size of the hash function, m is the message to be authenticated, the symbol shown as a '+' with a circle around it denotes an exclusive or (XOR) operation while the || denotes concatenation, and the outer padding opad=0x5c5c5c . . . 5c5c and inner padding ipad=0x363636 . . . 3636 are two one-block-long hexadecimal constants.

**[0097]** Thus, the secret key is the digital signature secret key known only to the secure computing module **200** and the user's financial organization **300**. The message to be authenticated is the financial transaction details along with a Transaction Number Identifier (TNI).

**[0098]** As an addition to the secure hash, a second secret encryption key may be optionally included and added to the list of items above for the financial transaction details, and, as a result, be included in the computation of the hashing function. This additional secret value will also be stored with the other keying material on the financial organization's secure computing module **200**. While keyed hashes are considered secure, cryptanalysts and hackers continue to make progress in breaking hashes and other encryption processes. To keep embodiments of the present invention more secure, this second secret key may be included in the hash function to increase the entropy of the computed secure hash in a manner that is easy for the secure computing modules **200** to process.

**[0099]** The TNI is a unique number associated with the current transaction and the secure computing module **200**. The unique number may be created in a number of ways. As a non-limiting example, the TNI may simply be a running incremented count of the transactions performed by the secure computing module **200**. As another non-limiting example, the TNI may be generated by a complex algorithm, such as a pseudo-randomly generated number, as long as the secure computing module **200** and the user's financial organization **300** can generate the same number for the current transaction.

**[0100]** Thus, the TNI refers to a counted or computed transaction number for a given party (e.g., buyer or seller) to a specific transaction and is created when the transaction is signed. The buyer and seller may have different transaction numbers as they will have performed a differing number of transactions or use a different TNI generation algorithm. In other embodiments, the TNI may be the same for both the buyer and the seller. In this case, the TMI will be computed by the party that initiates the transaction (either buyer or seller) and will be used in the digital signature process of the other party.

**[0101]** The TNI is included in the financial purchase package signing computation as part of the financial transaction details. It is also sent along with the signed FPP to the financial organization to help index the purchase transactions. Thus, there will most likely be a different TNI used by the buyer when the buyer signs the FPP than the TNI used by the seller when the seller signs the FPP.

**[0102]** It should be noted that the financial transaction details, along with the buyer's secure digital signature and the seller's secure digital signature may be transferred between the buyer's secure computing module **200**A and the seller's secure computing module **200**B over the proximate-field wireless communication channel **245**. The proximate-field communication wireless channel **245** may have a default frequency and protocol. As a non-limiting example, the proximate-field communication channel **245** may be RFID. However, another channel may be used if the default channel is not available, or the user selects a different channel for use. As non-limiting examples, other possible communication channels are Short Message Service (SMS), Multimedia Message Service (MMS), Wireless Application Protocol (WAP), Bluetooth, WiFi, and other suitable protocols.

**[0103]** In some cases, the proximate-field wireless communication channel **245** may not be particularly secure from snooping by others. However, embodiments of the present invention ensure that the current transaction is not compromised by using the secure digital signature of both the buyer and the seller. On the other hand, the financial transaction details may be discoverable if not encrypted, which may lead to identity theft if enough information is present in the financial transaction details. Consequently, some embodiments may include encryption and decryption of the financial purchase package. In addition, in some embodiments, the controlled content may be encrypted.

**[0104]** The encryption and decryption may use any suitable cryptographic algorithms. As a non-limiting example, the cryptographic algorithm may be a symmetric algorithm such as Advanced Encryption Standard (AES), which is well known in the art. Symmetric cryptography requires a secret key known only to the encryptor and the decryptor. Thus, the encryption may take place such that the secret key is known to a user and the user's financial organization. In this case, the secret key may be the same key used for creating the secure digital signature using the hashing algorithm, or it may be a different secret key used for the encryption/decryption. Alternatively, the secret key may be a secret key between the buyer and the seller determined during a discovery process, as is explained below.

**[0105]** As another non-limiting example, the cryptographic algorithm may be an asymmetric algorithm such as RSA, which is well known in the art. The RSA denotes initials of the individuals that first disclosed the encryption algorithm. In asymmetric cryptography, two keys are used, a public key and a private key. A user may let his public key be known to anyone and keeps his private key just to himself. Anyone wishing to send an encrypted message to the user encrypts the message using the user's public key. Once encrypted, the message can only be decrypted by the private key, which only the user knows.

**[0106]** Thus, there may be a number of keys stored and managed by the secure computing module **200**, such as, for example, secret digital signature keys, secret encryption keys, private keys, and public keys. Generally, users do not directly update their encryption and signing keys. In other words, users have access to use their keys but do not have access to manipulate their keys. Key updates, additions, or changes may be done by an organization controlling the servers that create the secure computing module **200**.

**[0107]** To manage and update keys securely, a Personal Identification Code (PIC) routine may be included in the secure computing module **200** to allow the user to authenticate himself to the secure computing module **200**. The PIC may include a series of alphanumeric values known only to the user and the secure computing module **200**. In another embodiment, the PIC may be the digital representation of some biometric feature such as a fingerprint or retinal scan. In another embodiment, the user may initiate a PIC input request wherein the secure computing module **200** outputs a series of alphanumeric characters that the user must in turn re-enter or re-type and submit back to the secure computing module **200**. Of course, the PIC routine may include combinations of entering biometric information and alphanumeric values. Furthermore, the PIC routine may include a random Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) algorithm for user entry. CAPTCHAs are the slanted and distorted fuzzy characters displayed that a human can discern, but which a computer may not be able to discern

**[0108]** In other embodiments, the secure computing module **200** may receive the PIC inputs directly from an attached or attachable input device (not shown). One example of this is an external fingerprint or retinal scan reader device that is connected via a wire(s) directly into the secure computing module **200**. This extra hardware provides more secure input that does not require the inputs to pass through the memory **506** or processor **502** of the host device **110** or other computing device containing the secure computing module **200**.

**[0109]** The secret keys for encryption/decryption as well as for secure hashing to create digital signatures may be refreshed periodically by the financial organization when the secure computing module **200** connects to the financial organization for transaction processing. If thus configured, the financial organization **300** may optionally initiate a connection to the host device **110** including the secure computing module **200** for the purpose of rekeying.

**[0110]** As a non-limiting example of used keys, two public and private key pairs may be created for each secure computing module **200**. For the first key pair, the public key is stored in the user's secure computing module **200** and the private key is stored with the financial organization's secure computing module **200**. This first key pair allows the user's secure computing module **200** to encrypt information to be sent to the financial organization. For the second key pair, the private key is stored in the user's secure computing module **200** and the public key is stored with the financial organization's secure computing module **200**. This second key pair allows the financial organization's secure computing module **200** to encrypt information to be sent to the user's secure computing module **200**. This two key pair system may be used so that each user's secure computing module **200** may have its own unique encrypted communication channel by which to communicate with the financial organization. Having separate keys for this purpose protects against a situation where if one encryption channel is hacked, then all encryption channels would be hacked. In addition, since public key encryption is much slower than symmetric key encryption, these two key pairs may be used to exchange a temporary symmetric key, which may be used for a specific transaction

**[0111]** Distribution of controlled content may occur with certain distribution rules and usage rules. The distribution rules specify how the content may be distributed. For example, distribution may be specified as unlimited. In another example, distribution may be specified as a certain quantity beyond which no further distribution is allowed. In another example, distribution may be limited to a specified time period, specific times, or select days.

**[0112]** In another example, distribution may be limited to certain distribution groups. In other words, distribution may be limited to individuals with memberships in specified groups. This allows a university professor, as a non-limiting example, to distributed text books or test notes to the current class and only the current class and not to the general public. This also allows companies to distribute "proprietary" material only to their employees and not to the community at large. Distribution group designations may be maintained on the secure computing module **200** and may also be verified during transactions with a distribution group's central repositories.

**[0113]** In the case of access authorization tokens, distribution may include distribution from the content owner, such as, for example, the venue owner, a ticket distributor, or other suitable event ticket seller. In addition, distribution, when authorized, may be between individuals. In this individual mode, distribution of access authorization tokens may be likened to a controlled ticket resale market.

**[0114]** In embodiments of the present invention, content owners may be financially compensated when the owner's controlled content is distributed. As a non-limiting example, a royalty fee may be preset at a certain amount or determined on a periodic basis. A periodic royalty may allow content owners to raise or lower purchase prices and royalty fees as dictated by market or other forces. For example, controlled content that is not selling, may sell better when its price is lowered by the content owner or content provider **350**. Conversely, a content owner may wish to raise the price of controlled content that is selling well. Dynamic pricing also allows for "sale days" or other periods where discounts are desired.

**[0115]** In addition, embodiments of the present invention enable content to be resold by a previous buyer. In a resale process, the content owner may collect a royalty for the additional distribution from the reseller to the buyer. In addition, if allowed by the distribution rules, resellers may collect a fee for themselves while also ensuring the specified royalty fee is paid to the content owner. If permitted by the distribution rules, the reseller fee may be negotiated between the reseller and the buyer.

**[0116]** In some embodiments, transfer restrictions and distribution rules may be set for a predetermined period of time. Further, the buyer's access to the controlled content may be limited to a predetermined period of time. After this predetermined period of time, the secure computing module may prevent access to the controlled content either by deleting, not decrypting, not allowing access, or combinations thereof.

**[0117]** In some embodiments, the secure computing module **200** may decrypt the controlled content and transfer it to the host device **110** for use. In other embodiments, the secure computing module **200** may retain the controlled content in the memory **230** of the secure computing module **200** and provide it to the host device **110** as requested.

**[0118]** To perform a financial transaction or controlled content distribution between two individuals with wireless communication devices, the secure computing modules **200** perform a discovery process such that the two secure computing modules **200** are aware of each other. When using portable

electronic devices, the discovery process take place over one of the proximate-field wireless communication channels (**245**B-**245**D).

**[0119]** In a wireless discovery process, an overt user selection from a host device **110** with a secure computing module **200** to initiate a transaction and connect to another host device **110**. This process is generally not simply "automatic" as in the case of most RFID payment cards and devices as the RFID process may be inherently insecure and prone to theft, eavesdropping, and abuse. However, in some embodiments, backward compatibility with conventional RFID systems, may be enabled to authorize automatic responses. As a non-limiting example, the use may switch to enable automatic responses for items such as low-dollar transactions such as subway fare transaction. As another non-limiting example, a conventional RFID system may be used to communicate an access authorization token from a secure computing module **200** to an admittance controller (not shown). The admittance controller may be operated by a venue to enable admittance to the venue access authorization token that are received by the admittance controller from one or more secure computing modules.

**[0120]** The discovery process may use any of several methods well known in the industry whereby an inquiry process looks for compatible devices. When such a device is found, both parties may input or negotiate the same secret session key value, etc. Session encryption may then based on that shared secret key value. Non-limiting examples of this discovery and key negotiation process are Bluetooth® pairing and enhancements to the Bluetooth® pairing process, which are well known in the art.

**[0121]** The discovery process may be conducted over the proximate-field wireless communicators **240** contained within the secure computing modules **200**. Having a secure processor control what, when, and how information is sent and received may enhance the security of the system.

**[0122]** Optionally, the discovery process may be conducted using conventional online client-server methods, or store and forward formats such as a secure Short Message Service (SMS) protocol.

**[0123]** FIG. **6** is a simplified flow diagram illustrating a process **600** that may be performed during distribution and purchase of controlled content from a content provider **350**. The process **600** may be followed with reference to FIG. **6**, and occasional reference to FIGS. **4** and **5**. It should be noted that any of the communications that occur between entities during process **600** may or may not be encrypted as is explained above.

**[0124]** The process **600** begins with the buyer selecting controlled content from a content provider **350** through the network at operation block **612**. The content provider **350** may be a variety of online distributors, such as, for example, iTunes, Amazon.com, Wal-Mart online, etc. In addition, the content provider **350** may be a physical store such as a Wal-Mart local store, a Best Buy local store, etc. The content provider **350** may also be a distribution kiosk in a local store or other facility. In process **600**, the content provider **350** may also be referred to as the seller **350**.

**[0125]** In operation block **614**, transaction details, the seller's credentials and the seller's digital signature are communicated from the seller **350** to the buyer's secure computing module **200**A. Along with the financial information of the transaction, the transaction details may include information about the content owner, the content owner's financial organization and distribution rules for the controlled content.

**[0126]** In operation block **616** the buyer is presented with a dialog box on the host device **110**A indicating the transaction details, distribution rules, and other pertinent information. The buyer is prompted to accept or deny the transaction. If the transaction is denied, process **600** stops (not shown). If the transaction is accepted, the buyer creates a financial purchase package including the transaction details, distribution rules and other information about the content, and the buyer's secure digital signature. The buyer then sends the financial purchase package back to the seller **350**.

**[0127]** If the seller or buyer does not approve and digitally sign the FPP, the process halts (not shown). If the transaction is to proceed, either the buyer or seller may send the financial purchase package on to a financial organization.

**[0128]** Decision block **620** determines if the seller is to communicate the FPP. If the seller communicates the financial purchase package, operation block **622** indicates that the seller sends the FPP to the seller's financial organization **300**B. In operation block **624**, the seller's financial organization **300**B authenticates the seller by examining the seller's secure digital signature.

**[0129]** This authentication process performs a reverse hashing process on the seller's digital signature using the seller's secret key and determines that the transaction details are accurate, the transaction number identifier is correct, and that the seller's credentials match the seller's account with this financial organization.

**[0130]** The seller's financial organization **300**B may then either approve or deny the transaction. If denied, the seller's financial organization **300**B sends a message back to the seller and the transaction terminates (not shown). If approved, the seller's financial organization **300**B sends the FPP and approval to the buyer's financial organization **300**A through the network **150**. In some cases, the buyer's financial organization **300**A and the seller's financial organization **300**B may be the same entity and there may be no need to "send" the FPP through the network **150**.

**[0131]** In operation block **626**, the buyer's financial organization **300**A authenticates the buyer by examining the buyer's secure digital signature using the buyer's secret key in a manner similar to that described above for the authentication process of the seller. The buyer's financial organization **300**A may then either approve or deny the transaction. If denied, the buyer's financial organization **300**A sends a message to the buyer's host device **110**A and the transaction terminates (not shown). If approved, the buyer's financial organization **300**A transfers the funds to the seller's financial organization **300**B.

**[0132]** Returning to decision block **620**, if the buyer communicates the financial purchase package, operation block **632** indicates that the buyer sends the FPP to the buyer's financial organization **300**A over the network **150**. In operation block **634**, the buyer's financial organization **300**A authenticates the buyer by examining the buyer's secure digital signature using the buyer's secret key as explained above.

**[0133]** The buyer's financial organization **300**A may then either approve or deny the transaction. If denied, the buyer's financial organization **300**A sends a message back to the buyer's host device **110**A and the transaction terminates (not shown). If approved, the buyer's financial organization **300**A sends the FPP and approval to the seller's financial organization **300**B through the network **150**. In some cases, the buyer's financial organization **300**A and the seller's financial organization **300**B may be the same entity and there may be no need to "send" the FPP through the network **150**.

**[0134]** In operation block **636**, the seller's financial organization **300**B authenticates the seller by examining the seller's secure digital signature using the seller's secret key as explained above. The seller's financial organization **300**B may then either approve or deny the transaction. If denied, the seller's financial organization **300**B sends a message to the seller **350** and the transaction terminates (not shown). If approved, the seller's financial organization **300**B sends the approval back to the buyer's financial organization **300**A. In operation block **638**, the buyer's financial organization **300**A transfers the funds to the seller's financial organization **300**B. At this point in the process, the financial transaction has been completed.

**[0135]** Decision block **640** determines whether the seller should be notified of the transaction results. If so, in operation block **642** the seller's financial organization **300**B sends the transaction results to the seller **350**.

**[0136]** Decision block **644** determines whether the buyer should be notified of the transaction results. If so, in operation block **646** the buyer's financial organization **300**A sends the transaction results to the buyer's secure computing modules **200**A.

**[0137]** Process block **648** indicates that the controlled content is communicated from the seller **350** to the buyer's secure computing module **200**A. As indicated earlier, the secure computing module may decrypt the controlled content if needed and store the controlled content in memory **230** on the secure computing module **200**A or transfer it to the host device **110**A.

**[0138]** In process **600**, any of the buyer's secure computing module **200**A, the seller **350**, the buyer's financial organization **300**A, and the seller's financial organization **300**B may keep a log of the financial transaction and its success or failure due to disapproval by any party or due to insufficient funds.

**[0139]** In process **600**, some of the communications may occur via an intermediary communication network such as the Internet, some communications may occur via cellular communication channels and some communications may occur via proximate-field wireless communication channels.

**[0140]** The financial organizations **300** include a secure computing module **200** and may employ an enterprise version of the secure computing module **200** software, hardware, or combination thereof. This enterprise version creates a secure mechanism that is more robust for numerous continuous and simultaneous transactions. To ensure additional security between transactions, the enterprise software for the secure computing module **200** may zero out dynamic transaction memory between individual transactions.

**[0141]** FIGS. **7**A and **7**B are simplified flow diagrams illustrating a process **700** that may be performed during distribution and purchase of controlled content between individuals. The process **700** may be followed with reference to FIGS. **7**A and **7**B, and occasional reference to FIGS. **4** and **5**. It should be noted that any of the communications that occur between entities during process **700** may or may not be encrypted as is explained above.

**[0142]** The process **700** begins with the reseller creating transaction details in operation block **702**. Along with the financial information of the transaction, the transaction details may include information about the content owner, the content owner's financial organization and distribution rules for the controlled content. The transaction details, the seller's credentials, and the seller's digital signature are communicated from the reseller's secure computing module **200**B to the buyer's secure computing module **200**A.

**[0143]** In operation block **704**, the buyer is presented with a dialog box on the host device **110**B indicating the transaction details, distribution rules, and other pertinent information. The buyer is prompted to accept or deny the transaction. If the transaction is denied, process **700** stops (not shown). If the transaction is accepted, the buyer's secure computing module **200**B creates a financial purchase package including the transaction details, distribution rules and other information about the content, and the buyer's secure digital signature. The buyer then sends the financial purchase package back to the reseller's secure computing module **200**A.

**[0144]** If the reseller or buyer does not approve and digitally sign the FPP, the process halts (not shown). In operation block **708**, the reseller's secure computing module **200**A sends the financial purchase package to the content owners financial organization **300**B and the buyer's financial organization **300**A.

**[0145]** In operation block **710**, the content owner's financial organization **300**B verifies the transaction details, the reseller's authorization to distribute and the distribution rules. In some cases, the content owner's financial organization **300**B may not know details of the reseller's authorization to distribute or the distribution rules. In those cases, the content owner's financial organization **300**B may communicate over the network **150** with the content owner or content provider **350** to verify the reseller's authorization to distribute and the distribution rules. If the transaction details and any content rules and authorization are verified, the content owner's financial organization **300**B may approve the transaction. Otherwise, the content owner's financial organization **300**B may deny the transaction. The content owner's financial organization then sends the approval or denial to the buyer's financial organization **300**A.

**[0146]** In operation block **712**, the buyer's financial organization **300**A verifies the transaction details and authenticates the buyer by examining the buyer's secure digital signature using the buyer's secret key as explained above.

**[0147]** The buyer's financial organization **300**A may then either approve or deny the transaction. If denied, the buyer's financial organization **300**A sends a message to the buyer's host device **110**A and the transaction terminates (not shown). If approved, the buyer's financial organization **300**A transfers the funds to the content owner's financial organization **300**B.

**[0148]** Referring to FIG. **7**B, in decision block **714**, the process determines whether the reseller is eligible to receive a fee for reselling the controlled content. If not, control passes down to decision block **724**.

**[0149]** If the reseller is to receive a fee, in operation block **718** the reseller sends the FPP to the reseller's financial organization (not shown, would be considered a third financial organization **300** in FIG. **5**).

**[0150]** In operation block **720**, the reseller's financial organization **300** authenticates the reseller by examining the reseller's secure digital signature using the reseller's secret key as explained above. The reseller's financial organization **300** may then either approve or deny the transaction. If denied, the reseller's financial organization **300** sends a message back to the reseller's host device **110**A and the transaction terminates (not shown). If approved, the reseller's financial organization **300** sends the FPP and approval to the buyer's financial organization **300**A through the network **150**. In some cases, the buyer's financial organization **300**A and

the reseller's financial organization **300** may be the same entity and there may be no need to "send" the FPP through the network **150**.

**[0151]** In operation block **722**, the buyer's financial organization **300**A transfers the funds for the reseller's fee to the reseller's financial organization **300**. At this point in the process, the financial transaction has been completed.

**[0152]** Decision block **724** determines whether the reseller should be notified of the transaction results. If so, in operation block **726** the reseller's financial organization **300** sends the transaction results to the reseller's secure computing module **200**A.

**[0153]** Decision block **728** determines whether the content owner, the content provider **350**, or combination thereof should be notified of the transaction results. If so, in operation block **730** the content owner's financial organization **300**B sends the transaction results to the content provider **350**.

**[0154]** Decision block **732** determines whether the buyer should be notified of the transaction results. If so, in operation block **734** the buyer's financial organization **300**A sends the transaction results to the buyer's secure computing module **200**A.

**[0155]** Process block **648** indicates that the controlled content is communicated from the reseller's secure computing module **200**A to the buyer's secure computing module **200**B. As indicated earlier, the secure computing module may decrypt the controlled content if needed and store the controlled content in memory **230** on the secure computing module **200**B or transfer it to the host device **110**B.

**[0156]** In process **700**, any of the buyer's secure computing module **200**B, the reseller's computing module **200**A, the buyer's financial organization **300**B, the reseller's financial organization **300**, and the content provider's financial organization **300**A may keep a log of the financial transaction and its success or failure due to disapproval by any party or due to insufficient funds.

**[0157]** In process **700**, some of the communications may occur via an intermediary communication network such as the Internet, some communications may occur via cellular communication channels, and some communications may occur via proximate-field wireless communication channels.

**[0158]** The financial organizations **300** include a secure computing module **200** and may employ an enterprise version of the secure computing module **200** software, which creates a secure mechanism that is more robust for numerous continuous and simultaneous transactions. To ensure additional security between transactions, the enterprise software for the secure computing module **200** may zero out dynamic transaction memory between individual transactions.

**[0159]** Although the present invention has been described with reference to particular embodiments, the present invention is not limited to these described embodiments. Rather, the present invention is limited only by the appended claims, which include within their scope all equivalent devices or methods that operate according to the principles of the present invention as described.

What is claimed is:

**1**. A secure computing module for operable coupling to a host device, comprising:

a processor for performing secure processing operations;

a host interface for operably coupling the processor to the host device; and

a memory operably coupled to the processor wherein the processor logically isolates at least some of the memory from access by the host device;

wherein the secure computing module is configured to:

generate a secure digital signature for a message including financial transaction details;

direct the host device to communicate the financial transaction details and the secure digital signature to a financial organization associated with a user of the secure computing module; and

enable controlled content received through the host device.

**2**. The secure computing module of claim **1**, wherein the secure digital signature comprises a secure hash function generated using a secret key on a message comprising the financial transaction details and a transaction number identifier.

**3**. The secure computing module of claim **1**, wherein the secure computing module is further configured to encrypt the financial transaction details, the secure digital signature, or combination thereof in isolation from the host device and prior to directing the host device to communicate the financial transaction details and the secure digital signature.

**4**. The secure computing module of claim **3**, wherein the encryption is performed with a symmetric encryption process using a secret key known by the secure computing module and the financial organization associated with the user.

**5**. The secure computing module of claim **3**, wherein the encryption is performed with an asymmetric encryption process using a public key associated with the financial organization.

**6**. The secure computing module of claim **1**, wherein the host device is selected from the group consisting of cell phones, smartphones, pagers, Personal Digital Assistants, handheld computing platforms, wrist-worn computing systems, mobile computing systems, and desktop computing systems.

**7**. The secure computing module of claim **1**, wherein the secure computing module is further configured to decrypt the controlled content for use by the host device.

**8**. The secure computing module of claim **1**, further comprising a proximate-field wireless communicator operably coupled to the processor and configured for communication with another secure computing module associated with another host device when within a proximate-field range of the other secure computing module.

**9**. The secure computing module of claim **8**, wherein the proximate-field wireless communicator is configured to communicate using available radio frequencies, infrared frequencies, 802.1 a/b/g/n type wireless connections, Bluetooth, RFID, WiFi, WiMax, or combinations thereof.

**10**. The secure computing module of claim **8**, wherein the secure computing module uses the proximate-field wireless communicator to communicate the financial transaction details and the secure digital signature to the other secure computing module.

**11**. A method of performing file distribution, comprising:

selecting controlled content to be received from a content provider acting as a seller;

sending financial transaction details for the controlled content to a buyer;

signing the financial transaction details with a buyer's secure digital signature using a buyer's secure computing module;

signing the financial transaction details with a seller's secure digital signature using a seller's secure computing module, wherein the financial transaction details, the buyer's secure digital signature, and the seller's secure digital signature comprise a financial transaction package;

communicating the financial transaction package between the buyer and the seller;

communicating the financial transaction package to a seller's financial organization;

communicating the financial transaction package to a buyer's financial organization;

from the seller's financial organization:

verifying the seller's secure digital signature and the financial transaction details; and

sending a seller approval to the buyer's financial organization; and

from the buyer's financial organization:

verifying the buyer's secure digital signature and the financial transaction details;

sending a buyer approval to the seller's financial organization; and

performing a fund transfer from the buyer's financial organization to the seller's financial organization; and

communicating the controlled content from the content provider to the buyer's secure computing module.

**12**. The method of claim **11**, further comprising preventing the performing the fund transfer when the verifying the buyer's secure digital signature and the financial transaction details is not successful or when the verifying the seller's secure digital signature and the financial transaction details is not successful.

**13**. The method of claim **11**, further comprising encrypting the financial transaction details, the buyer's secure digital signature, the seller's secure digital signature, or combinations thereof prior to at least one of the communicating acts.

**14**. The method of claim **11**, further comprising decrypting the controlled content after the communicating the controlled content.

**15**. The method of claim **11**, wherein verifying the financial transaction details comprise verifying a transaction amount, a buyer's credentials, a seller's credentials, or a combination thereof.

**16**. The method of claim **11**, wherein signing the financial transaction details with the buyer's secure digital signature comprises performing a secure hash function using a buyer's secret key on a message comprising the financial transaction details and a buyer's transaction number identifier.

**17**. The method of claim **11**, wherein signing the financial transaction details with the seller's secure digital signature comprises performing a secure hash function using a seller's secret key on a message comprising the financial transaction details and a seller's transaction number identifier.

**18**. The method of claim **11**, further comprising communicating a transaction results to at least one of a buyer's host device or a seller's host device.

**19**. The method of claim **11**, wherein communicating the controlled content comprises communicating an access authorization token.

**20**. The method of claim **19**, further comprising communicating the access authorization token from the buyer's secure computing module to an admittance controller to enable admittance of the buyer.

**21**. A method of performing file distribution, comprising:

selecting controlled content to be received from a reseller;

determining financial transaction details including a transaction amount and a content owner for the controlled content;

sending the financial transaction details for the controlled content to a buyer;

signing the financial transaction details with a buyer's secure digital signature using a buyer's secure computing module;

signing the financial transaction details with a reseller's secure digital signature using a reseller's secure computing module, wherein the financial transaction details, the buyer's secure digital signature, and the reseller's secure digital signature comprise a financial transaction package;

communicating the financial transaction package between the buyer and the reseller;

communicating the financial transaction package to a buyer's financial organization;

communicating the financial transaction package to a content owner's financial organization;

from the content owner's financial organization:

verifying the financial transaction details and sending a seller approval to the buyer's financial organization

from the buyer's financial organization:

verifying the buyer's secure digital signature and the financial transaction details;

sending a buyer approval to the content owner's financial organization; and

performing a fund transfer from the buyer's financial organization to the content owner's financial organization; and

communicating the controlled content from the reseller's secure computing module to the buyer's secure computing module.

**22**. The method of claim **21**, further comprising:

communicating the financial transaction package to a reseller's financial organization;

from the reseller's financial organization:

verifying the reseller's secure digital signature and the financial transaction details; and

sending a reseller's approval to the buyer's financial organization; and

performing another fund transfer from the buyer's financial organization to the reseller's financial organization.

**23**. The method of claim **21**, further comprising preventing the performing the fund transfer when the verifying the buyer's secure digital signature and the financial transaction details is not successful.

**24**. The method of claim **21**, further comprising encrypting the financial transaction details, the buyer's secure digital signature, the reseller's secure digital signature, or combinations thereof prior to at least one of the communicating acts.

**25**. The method of claim **21**, wherein determining the financial transaction details comprises determining a transaction amount, a buyer's credentials and a reseller's credentials.

**26**. The method of claim **21**, wherein signing the financial transaction details with the buyer's secure digital signature comprises performing a secure hash function using a buyer's secret key on a message comprising the financial transaction details and a buyer's transaction number identifier.

**27**. The method of claim **21**, wherein signing the financial transaction details with the reseller's secure digital signature

comprises performing a secure hash function using a reseller's secret key on a message comprising the financial transaction details and a reseller's transaction number identifier.

**28**. The method of claim **21**, wherein communicating the financial transaction package between the buyer and the reseller comprises communicating between the buyer's secure computing module and the reseller's secure computing module via a proximate-field wireless communication channel.

**29**. The method of claim **28**, wherein communicating via the proximate-field wireless communication channel comprises communicating using available radio frequencies, infrared frequencies, 802.1 a/b/g/n type wireless connections, Bluetooth, RFID, WiFi, WiMax, or combinations thereof.

**30**. The method of claim **21**, further comprising communicating a transaction results to at least one of a buyer's host device, a content owner's host device, or a reseller's host device.

**31**. The method of claim **21**, wherein communicating the controlled content comprises communicating an access authorization token.

**32**. The method of claim **31**, further comprising communicating the access authorization token from the buyer's secure computing module to an admittance controller to enable admittance of the buyer.

**33**. A system for performing file distribution, comprising:

a first host device associated with a buyer of controlled content and including a first secure computing module operably coupled thereto, the first secure computing module configured to:

generate a buyer's secure digital signature for a message including financial transaction details;

direct the first host device to communicate the financial transaction details and the secure digital signature to a buyer's financial organization and to a second secure computing module; and

communicate the controlled content to the second secure computing module; and

a second host device associated with a seller of the controlled content and including the second secure computing module operably coupled thereto, the second secure computing module configured to:

generate a seller's secure digital signature for the message;

direct the second host device to communicate the financial transaction details and the secure digital signature to a seller's financial organization and to the first secure computing module; and

receive the controlled content from the second secure computing module.

* * * * *