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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 August 2009 (27.08.2009)

PCT

(10) International Publication Number
WO 2009/105302 A1

(51) International Patent Classification:
H04L 9/32 (2006.01) *G06Q 30/00* (2006.01)
G06F 21/20 (2006.01)

(21) International Application Number:
PCT/US2009/031451

(22) International Filing Date:
20 January 2009 (20.01.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
12/035,531 22 February 2008 (22.02.2008) US

(71) Applicant *(for all designated States except US)*: **MICROSOFT CORPORATION** [US/US]; One Microsoft Way, Redmond, Washington 98052-6399 (US).

(72) Inventors: **SHEN, Hui**; c/o Microsoft Corporation, One Microsoft Way, Redmond, Washington 98052-6399 (US). **HASSAN, Amer, A.**; c/o Microsoft Corporation, One Microsoft Way, Redmond, Washington 98052-6399 (US). **LU, Yi**; c/o Microsoft Corporation, One Microsoft Way, Redmond, Washington 98052-6399 (US). **KUEHNEL, Thomas, W.**; c/o Microsoft Corporation, One Microsoft Way, Redmond, Washington 98052-6399 (US). **BARON, Andrew, T.**; c/o Microsoft Corporation, One Microsoft Way, Redmond, Washington 98052-6399 (US). **WU, Deyun**; c/o Microsoft Corporation, One Microsoft Way, Redmond, Washington 98052-6399 (US).

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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR),

[Continued on next page]

(54) Title: AUTHENTICATION MECHANISMS FOR WIRELESS NETWORKS

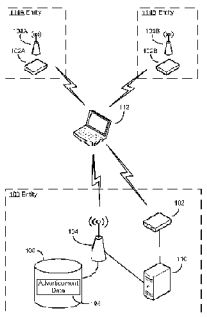

FIG. 1A

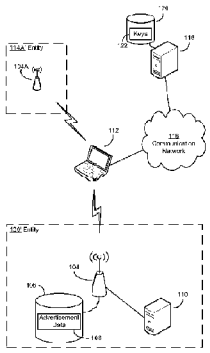

FIG. 1B

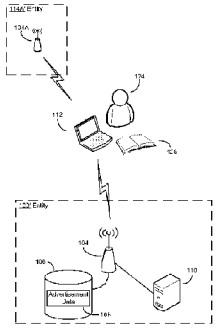

FIG. 1C

(57) Abstract: Security techniques and security mechanisms for wireless networks that transmit content such as advertisements. According to exemplary techniques, control messages comprising unrequested content (e.g., advertisement data) may be transmitted in response to request from a client device, while in other exemplary techniques control messages may be transmitted without any request from a client device. In some exemplary implementations, security mechanisms such as public key cryptography algorithms may be used to secure transmissions. In some of these techniques which implement public key cryptography, user may be required to retrieve a public key from a source other than the wireless access point transmitting encrypted advertisements (e.g., a sign or terminal in a commercial entity transmitting such advertisements, or from a web service), such that user may confirm that the encrypted content is from a source matching the retrieved public key and thus confirm the authenticity of a wireless access point.

WO 2009/105302 A1

OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

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

Published:

— *with international search report (Art. 21(3))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

AUTHENTICATION MECHANISMS FOR WIRELESS NETWORKS

BACKGROUND OF INVENTION

Conventional web-based advertising frameworks typically transmit advertisements to consumers of a web-based service through a connection that the client device has established, through a network, to a server hosting the web-based service. For example, the owner/administrator of a server may configure the server to transmit to the client device a web page with an advertisement in response to a user of a client device entering a Uniform Resource Locator (URL) into the client device. The advertisement may be in the form of text/image/video/audio data and may be embedded in the web page, or may be an initial web page to be displayed to the user prior to displaying the web page accessed by the client device.

In such advertising frameworks, advertisements are exchanged between a web-based service (e.g., a web site) and users of the web-based service. The network to which a user's client device connects and through which the client device accesses the web-based service has limited involvement in controlling the content of the web page and thus has limited capability to provide advertisements to a user of the client device. Instead, some networks implement alternative, complementary advertising frameworks, for example, ones which transmit web pages containing advertisements to users of client devices connected to the network. The advertising frameworks implemented by these networks, for example, may require a user of the network to view an initial web page when first connecting to the network, or may periodically transmit web pages containing advertisements to client devices using the network.

SUMMARY OF INVENTION

Conventional advertising frameworks for wireless networks are limited in their ability to transmit advertisements to users, as the advertisements may only be transmitted to client devices with an established connection to the wireless network and/or which are requesting data from the wireless network. If advertisements could be transmitted to client devices not connected to a wireless network, then the advertisements may reach more users and advertising businesses may draw more customers and more revenue.

Enabling client devices to accept openly unrequested content from networks to which they are not connected, however, may open users of the devices to various risks.

For example, undesirable advertisements (e.g., pornographic advertisements) may be transmitted by a organization in which a user is not interested, or by a malicious party masquerading as an organization in which the user is interested. Without any security mechanisms and/or methods of identifying the networks transmitting advertisements and other content, such undesirable advertisements may be received by a client device and displayed to the user and may cause offense or outrage to the user.

Frameworks other than advertising frameworks may also benefit from being able to transmit unrequested content to client devices and, in turn, these client devices may benefit from security mechanisms and/or methods of identifying networks transmitting unrequested content. For example, wireless access points may transmit location data for themselves to client devices tracking their own locations, and confirming the identity of these wireless access points may prevent malicious parties from broadcasting fraudulent location data.

Disclosed herein are various principles for security techniques and security mechanisms for wireless networks which transmit content such as advertisements. According to some of the exemplary techniques, control messages comprising unrequested content (e.g., advertisement data) may be transmitted in response to a request from a client device, while in other exemplary techniques the control messages may be transmitted without any request from a client device. In some exemplary implementations, security mechanisms such as public key cryptography algorithms may be used to secure transmissions. In some of these techniques which implement public key cryptography, a user may be required to retrieve a public key from a source other than the wireless access point transmitting encrypted advertisements (e.g., a sign or terminal in a commercial entity transmitting such advertisements, or from a web service), such that the user may confirm that the encrypted content is from a source matching the retrieved public key and thus confirm the authenticity of a wireless access point.

In one embodiment, there is provided a method of operating a client device to display advertisement information relating to a commercial service. The method comprises obtaining trust information for a wireless access point, verifying, based on the trust information, the authenticity of a control transmission from the wireless access point, and selectively displaying to a user an advertisement for at least one commercial service contained within the control message based at least in part on the act of verifying.

In another embodiment, there is provided at least one computer-readable medium encoded with computer-executable instructions which, when executed, cause a computer to execute a method for confirming authenticity of a control transmission from a wireless access point associated with an entity. The method comprises obtaining trust information for the entity, verifying, using the trust information, the authenticity of a control transmission from the wireless access point, and selectively using contents of the control transmission based at least in part on the act of verifying.

In a further embodiment, there is provided an apparatus for transmitting control messages in a wireless network. The apparatus comprises at least one data store storing trust information and contents, at least one processor adapted to construct a control transmission comprising the contents and to encrypt at least a portion of the control transmission using the trust information, and a communication circuit to transmit the control transmission.

BRIEF DESCRIPTION OF DRAWINGS

The accompanying drawings are not intended to be drawn to scale. In the drawings, each identical or nearly identical component that is illustrated in various figures is represented by a like numeral. For purposes of clarity, not every component may be labeled in every drawing. In the drawings:

FIG. 1A is a diagram of an exemplary computer system in which some, but not all, of the techniques disclosed herein for transmitting, receiving, and verifying the authenticity of control messages may act, the computer system comprising kiosks from which trust information for entities may be read;

FIG. 1B is a diagram of an exemplary computer system in which some, but not all, of the techniques disclosed herein for transmitting, receiving, and verifying the authenticity of control messages may act, the computer system comprising a web server hosting a web site from which trust information may be retrieved;

FIG. 1C is a diagram of an exemplary system in which some, but not all, of the techniques disclosed herein for transmitting, receiving, and verifying the authenticity of control messages may act, the system comprising a paper directory from which trust information may be retrieved;

FIG. 2 is a flowchart of an illustrative process implementing some of the principles disclosed herein that may be implemented by a computer system for exchanging information about a commercial service between a wireless network and a client device;

FIG. 3 is a flowchart of one exemplary technique implementing some of the principles disclosed herein for confirming the authenticity of a wireless access point of a wireless network;

FIG. 4 is a flowchart of one exemplary technique implementing some of the principles disclosed herein for confirming the authenticity of control messages received from a wireless access point of a wireless network;

FIG. 5 is a flowchart of another exemplary technique implementing some of the principles disclosed herein for confirming the authenticity of control messages received from a wireless access point of a wireless network;

FIG. 6 is a flowchart of an exemplary technique implementing some of the principles disclosed herein which may be used by wireless access points to transmit control messages;

FIG. 7 is a block diagram of an exemplary wireless access point which may implement some, but not all, of the techniques disclosed herein for transmitting and verifying the authenticity of control messages; and

FIG. 8 is a block diagram of an exemplary client device which may implement some, but not all, of the techniques disclosed herein for receiving and verifying the authenticity of control messages received from wireless access points of wireless networks.

DETAILED DESCRIPTION

Applicants have appreciated that both businesses and consumers may benefit from a simple mechanism for making computer-based advertisements available to consumers in close proximity, for example, to the locations at which advertised services are available. For example, users may learn of sales or special promotions offered by a business. Also, the user can learn about services offered by a business to determine that the user is interested in the services offered by the business before entering the premises for that business.

Conversely, advertisers may focus advertisements on potential customers who are near their establishments and therefore most likely to make purchases. For example, a

restaurant having a wireless network may seek to draw more customers by transmitting to client devices within range a description of the restaurant's daily specials. Conventional advertising frameworks cannot deliver advertisements in this fashion. While capable of transmitting advertisements to large numbers of users, conventional frameworks are limited to displaying advertisements to users of client device already connected to a wireless network through a wireless access point who request data from the wireless network. Such conventional frameworks are not capable of displaying advertisements to users not connected to the wireless network or alerting users who do not know to request information that advertisements are available for businesses in close proximity to the user.

Applicants have appreciated the desirability of advertising services of a business, including services such as selling one or more products, to users of client devices not connected to a wireless network operated by the business. If businesses were capable of advertising their products or services to all client devices within range of their wireless networks, rather than just client devices connected to the wireless networks, then the advertisements would be able to reach a wider audience and the business might attract more customers and more revenue. Further, users of client devices within range of the wireless network are the most likely group of potential customers because of their proximity to the business when they receive the transmitted advertisements.

Applicants have additionally appreciated, however, that enabling client devices to receive openly content from nearby networks and displaying that content to a user without verifying the authenticity of the networks and/or content opens the user to various risks. For example, advertisements in which a user is not interested may be displayed, and/or advertisements which are offensive to a user may be displayed. For example, a user walking through a shopping mall may walk within range of a business selling goods that the user finds undesirable (e.g., pornography) and the user may find any advertisement for the business undesirable or offensive. Further, if a client device displays all received advertisements to a user, then a malicious third party may set up a fraudulent wireless network and transmit advertisements that appear to be for a legitimate source but which are actually offensive or undesirable images and/or text that the client device would automatically display to a user.

Additionally, Applicants have appreciated that frameworks other than advertising frameworks may benefit from transmitting unrequested content through wireless networks to client devices and that those client devices may benefit from confirming the identity of

those networks prior to accepting the content. For example, a wireless access point broadcasting data indicating the location of the wireless access point may be helpful to a client device, within range of the wireless access point, attempting to ascertain its own location. Without any techniques in place for confirming the identity of wireless access points and/or wireless networks, however, the client device, in this scenario, is open to accepting fraudulent location data from a malicious third party. Other frameworks that exchange information wirelessly with client devices may similarly benefit from the techniques disclosed herein.

Applicants have therefore appreciated that desirability of security mechanisms for wireless networks to enable client devices to confirm the identity of wireless networks prior to accepting unrequested information from the wireless networks. Security mechanisms may permit a user and/or a client device to verify the authenticity of a control message from a wireless access point containing content (e.g., an advertisement, location data, or other information). Alternatively or additionally, the security mechanisms may be used to verify the authenticity of a wireless network comprising one or more wireless access points transmitting control messages, or any other component of any suitable framework before content is displayed to the user. Additionally, security mechanisms may permit a user to limit content the user wishes the client device to use (e.g., the content selected to be displayed to the user).

In view of the foregoing, techniques have been devised which are directed to security mechanisms for confirming the identity of wireless networks. In one exemplary technique, a user receives trust information for one or more commercial entities, verifies the authenticity of one or more control transmissions or network components using the trust information, and selectively displays content contained in the one or more control transmissions from those commercial entities based on the success of the verification.

Any suitable transmission may be a control transmission in accordance with one or more of the principles described herein. For example, layer 2 control transmissions such as announcement transmissions may comprise any suitable information about a wireless access point, including one or more network characteristics enabling a client device receiving the control transmission to open a connection to the wireless access point. An announcement transmission may be, for example, a beacon in accordance with an Institute of Electrical and Electronics Engineers (IEEE) 802.11 wireless protocol periodically broadcast by a wireless access point to all client devices within range of the wireless

access point, a probe response transmitted to a client device in response to a request for control information sent by the client device, or any other suitable announcement transmission sent by a wireless access point. Control transmissions sent by a client device to a wireless access point may be any suitable transmission, such as a probe requesting control information about the wireless access point and/or wireless network which may or may not comprise test data, an authentication test message of any suitable type, and/or any other suitable transmission.

In some, but not all, implementations of the techniques described herein the security techniques may be implemented as a one- or two-way public key encryption algorithm. In implementations which do use public key encryption, any suitable public key algorithm may be used, such as the popular Rivest-Shamir-Adleman (RSA) public key algorithm, though the invention is not limited to implementing any particular security technique or any particular public key algorithm.

In some implementations, such as those implementing public key cryptography, a user or a client device may obtain trust information from an "out of band" source (i.e., a source other than through the wireless network itself) such as a book, sign, key service, electronic key provider, a kiosk or other device communicating using one or more protocols such as the Near-Field Communication (NFC) protocol, or any other suitable source. The trust information may be, in some implementations, a public key associated with a wireless network or wireless access point and/or a Public Key Infrastructure (PKI) certificate approved by a certificate authority. As described in greater detail below, a client device having trust information for a wireless network or wireless access point may use the trust information in any suitable manner to confirm the identity of the wireless access point and/or wireless network.

For example, in some techniques implementing some of the principles described herein, a wireless access point may transmit control transmissions encrypted using a private key corresponding to a public key retrieved by the client device as part or all of the trust information. In some implementations, the control transmissions may be entirely encrypted, while in alternative transmissions only a portion or all of the control transmission payload (e.g., contents such as advertisement data, or information elements comprising one or more pieces of content) are transmitted. If the client device is able to correctly decrypt the control message using the public key, the client device can confirm that the control message was encrypted using a private key corresponding to the retrieved

public key and, accordingly, the wireless access point transmitting the encrypted control message is the wireless access point from which the client device expected to receive information.

Additionally or alternatively, in some implementations, the client device may exchange one or more test transmissions as control transmissions to test the authenticity of a wireless access point and/or wireless network. For example, a client device may encrypt test data using the trust information (e.g., the retrieved public key) and transmit the encrypted test data to the wireless access point. If the control transmission received from the wireless access point in response to the test transmission contains the correct test data, then the client device can confirm that the wireless access point was able to correct decode the transmission, and as such the wireless access point has the private key corresponding to the public key and is the wireless access point with which the client device expected to communicate. Greater security may be provided by adding other information to the test data. This other information may be any suitable information, such as a public key of a client device, and replies sent by the wireless access point may be sent encrypted using the public key of the client device. Alternatively, the test data could be a nonce or other unique symbol (e.g., unique text or a transmission time) so that even if a control transmission from a wireless access point is intercepted, recorded, and rebroadcast from a hoax device (to make the hoax device appear authentic), the client device may detect that the control transmission is being "replayed" by using one or more techniques for avoiding reply attacks, such as by noting the repetition of what should have been a unique symbol or an unusual delay in the transmission time (i.e., an extreme difference between a current time and the claimed transmission time of the control transmission may imply that the control transmission had been recorded at the transmission time and rebroadcast by a hoax device at a later time).

It should be appreciated that these techniques are merely illustrative of techniques that may implement the principles described herein, and that the principles described herein for confirming the identity of wireless networks may be implemented in any suitable manner using any suitable security mechanism, as the invention is not limited in this respect.

It should be additionally appreciated that control transmissions may be formatted in any suitable manner to contain any suitable type or types of contents (e.g., advertisement data and/or location data). Exemplary techniques for encapsulating contents

in information elements of control transmissions are discussed in co-pending applications 11/973,589 ("Advertising framework for wireless networks") and 11/973,590 ("Transmitting location data in wireless networks"). These applications describe using, among other formats, information elements of the IEEE 802.11 wireless communication protocol to include advertisement and location data in control transmissions such as beacons and probe responses. The principles described herein, however, may be implemented using any suitable control transmission incorporating contents in any suitable manner, and are not limited to the techniques discussed therein.

The techniques described herein may be implemented in any suitable system comprising one or more wireless networks, each comprising one or more wireless access points and any suitable means for the client device to obtain trust information for wireless networks, as the invention is not limited in this respect. Described below are three exemplary systems which implement some of the principles described herein.

FIG. 1A shows an exemplary system in which some of the techniques disclosed herein may act. It should be appreciated that embodiments of the invention may act in any suitable system and are not limited to being implemented in the illustrative system shown in FIG. 1A.

The system of FIG. 1A comprises an exemplary client device 112 within range of three wireless access points 104, 104A, and 104B. Each of the wireless access points shown in FIG. 1A is associated with an entity, such as entity 100, entity 114, and entity 116. In some embodiments of the invention, an entity may be a commercial entity such as a business, collection or association of businesses, non-profit/public organization, or other commercial entity, though it should be appreciated that embodiments of the invention are not limited to be implemented with commercial entities. It should be additionally appreciated that, as used herein, an "entity," including a commercial entity, may be any single entity, such as a person, group, organization, or business, or any combination of persons, groups, organizations, businesses, or any other entities which may be associated with one another in any suitable manner (e.g., as a business association or a group of businesses sharing infrastructure such as in a shopping mall). It should be appreciated that while various examples are described below in which, for clarity, the entity is described as a commercial entity such as a business or shopping mall, the invention is not limited to being implemented with any particular type or types of entities.

FIG. 1A shows in entity 100 an exemplary implementation of an entity (including entities such as entities 114A and 114B) in accordance with embodiments of the invention. An entity may comprise at least one wireless access point 104, which may be communicatively coupled to a data store 106 and a server 110 associated with the wireless access point 104. Data store 106 may be any suitable computer-readable medium, and may be a component of the wireless access point 104, or may be coupled to the wireless access point 104 directly or through any suitable wired and/or wireless communication medium or media. As shown in FIG. 1A, in some implementations, data store 106 may store information comprising advertisement data that may be retrieved and transmitted by the wireless access point 104. The advertisement data 108 may be any suitable type or types of data that may be transmitted by a wireless access point 104, including, for example, data describing text, images, audio, or video, or any combination thereof. The advertisement data 108 may be data describing a single advertisement for one or more services associated with the entity 100, or may be data describing multiple advertisements for one or more services associated with the entity 100. It should be appreciated that, as discussed above, advertisement data is merely illustrative of the types of data that may be transmitted by wireless access points of wireless networks, and that any suitable type or types of information may be transmitted, as the invention is not limited in this respect.

Server 110 may be any suitable computing apparatus for storing information (e.g., data and/or instructions) to be provided to a client device connected to wireless access point 104. While FIG. 1 shows server 110 as separate from wireless access point 104 and data store 106, in some embodiments of the invention, server 110 may be a component of wireless access point 104 and/or may be implemented as an electronic device comprising a computer-readable medium (or computer-readable media) acting as both a server 110 and a data store 106. In the embodiment illustrated, server 110 is connected to a network that a device may access once it associates with wireless access point 104 and gains access to that network. However, it should be appreciated that the system of FIG. 1A is merely exemplary, and that it is not a requirement of the invention that a wireless access point providing advertising data or other contents ultimately support connections to other networked devices.

The information stored by server 110 may comprise, in some implementations, information related to the one or more advertisements described by the advertisement data 108 stored by data store 106. The information related to the one or more advertisements

may be any suitable information, including, for example, one or more web pages describing one or more product(s) or service(s) being advertised by the advertisement data 108. In the embodiments illustrated, data store 106 may not fully define contents of advertisements described by the advertisement data 108. However, such advertisements, for example, may contain a URL pointing to server 110 such that a user may select to connect through wireless access point 104 or any other suitable network connection to server 110 to obtain information related to an advertised service.

Wireless access point 104 may be any suitable wireless signal generator generating signals according to one or more wireless networking protocols. For example, the wireless access points may be WiFi access points operating according to the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standard for Wireless Local Area Networks (WLANs), may be cellular-style wireless access points operating a Wireless Wide Area Network (WWAN) according to any suitable WWAN protocol (e.g., the Global System for Mobile Communications (GSM)), personal area network (PAN) protocols such as Bluetooth, other protocols such as the Worldwide Interoperability for Microwave Access (WiMAX) protocol and the Ultra-wideband (UWB) protocol, or any other suitable wireless protocol. In an entity having multiple wireless access points, the wireless access points may be operating according to the same wireless protocol or may be operating according to different wireless protocols.

As discussed above, systems implementing some of principles disclosed herein may have methods for obtaining trust information for wireless access points and wireless networks other than through the wireless access points and wireless networks themselves (i.e., an out of band source). In some non-preferred implementations, the trust information may be retrieved from the wireless network itself, but it should be appreciated that out of band sources are preferred.

In the embodiment of the FIG. 1A, entity 100 is equipped with a kiosk 102 from which a client device may retrieve trust information. The kiosk 102 may be, for example, an electronic device located within or in proximity to the entity 100. In some implementations, the kiosk 102 may be a device mounted at the entrance to a business or the entrance of a shopping mall, or at locations throughout the business or shopping mall (e.g., mounted on a pillar or wall), which the user may access to retrieve one or more pieces of trust information for that business or shopping mall. The client device 112 may communicate with the kiosk 102 to retrieve the trust information in any suitable manner.

In some implementations, the client device 112 may communicate with the kiosk 102 using any suitable wireless protocol, such as a WLAN or PAN protocol or using any suitable Near Field Communication (NFC) protocol (e.g., Radio Frequency Identification (RFID) techniques), or using any suitable wired or contact-based communication techniques. For example, in some implementations, a user may retrieve from the kiosk 102 a memory unit (e.g., a memory card) to be inserted into the client device 112 from which the client device 112 may copy trust information or which the user may keep while shopping at the business or shopping mall (or otherwise interacting with an entity). As discussed above, the trust information retrieved from the kiosk 102 may be any suitable trust information, such as a public key or a PKI certificate for the entity 100.

As shown in FIG. 1A, a client device 112 receiving transmissions from one or more wireless access points 104, 104A, and 104B, may be a laptop personal computer. It should be appreciated, however, that embodiments of the invention are not limited to be implemented with a laptop personal computer, and may be implemented with any suitable electronic device for receiving wireless signals, mobile or immobile, such as a desktop or laptop personal computer, a personal digital assistant (PDA), or smart phone.

The client device 112 may or may not have a connection open to one or more wireless access points 104, 104A, and 104B, but is within range of each of the wireless access points 104, 104A, and 104B and is capable of receiving transmissions from the wireless access points 104, 104A, and 104B. As discussed above, in accordance with embodiments of the invention the transmissions received from the wireless access points 104, 104A, and 104B may comprise any suitable information, including advertisement data 108 stored by the data store 106. In accordance with some illustrative techniques, the transmissions sent by the wireless access points 104, 104A, and 104B and received by the client device 112 may be layer 2 control transmissions. Layer 2 control transmissions such as announcement transmissions may comprise any suitable information about the wireless access point 104, including one or more network characteristics enabling a client device receiving the control transmission to open a connection to the wireless access point 104. As discussed above, an announcement transmission may be, for example, a beacon in accordance with an IEEE 802.11 wireless protocol periodically broadcast by a wireless access point 104 to all client devices within range of the wireless access point 104 (including client device 112), a probe response transmitted to a client device 112 in

response to a request for control information sent by the client device 112, or any other suitable announcement transmission sent by a wireless access point 104.

In some embodiments of the invention, a wireless access point 104 may encode in a control transmission the advertisement data 108 stored by the data store 106. As discussed in greater detail below, a client device 112 may be adapted to receive the control transmission comprising content (e.g., the advertisement data 108 or any other suitable content) and read from the control transmission the content. Once read, the content may be processed in any suitable manner, such as providing the advertisements described by the advertisement data 108 to a user of the client device 112 through any suitable user interface. In some advertising frameworks which may implement the techniques described herein for security, a user may then view the advertisements and may indicate to the client device 112 that he or she desires more information on the products or services described by the advertisements. The client device may then establish a connection to a wireless access point transmitting the advertisement in which the user indicated he or she was interested (if the client device 112 does not already have an open connection to the wireless access point), and retrieve any suitable additional information about the one or more services described by the advertisement. The additional information may comprise one or more web pages containing more information about the services or one or more web pages from which the user may order or subscribe to the services. It should be appreciated, however, that in some advertising frameworks implementing the techniques described herein the additional information may not be one or more web pages and may instead be any suitable additional information that may be provided to a user of a client device.

It should be appreciated that the exemplary computer system in FIG. 1A is merely illustrative, and that embodiments of the invention may act in any suitable computer system comprising any suitable number of client devices, entities, and wireless access points. Further, it should be appreciated that entities and wireless access points are not limited to being implemented as shown in the example of FIG. 1A, as embodiments of the invention may be implemented with any suitable entity employing any suitable hardware and/or software.

FIGs. 1B and 1C show alternative systems in which techniques implementing some of the principles described herein may act. As shown in FIGs. 1B and 1C, entities 100' and 114A' are substantially similar as the entities shown in FIG. 1A, but the entities

are not shown comprising a kiosk 102. Rather, in FIG. 1B, a server 116 is shown communicatively connected to the client device 112 through a communication network 118 comprising any suitable wired and/or wireless communication medium or media. Server 116 may be a server for providing trust information for one or more entities in any suitable manner, such as through a web site or web service, such as the MSN or Windows Live services available from the Microsoft Corporation of Redmond, Washington, that may act as a certificate authority for issuing PKI certificates and/or as a repository for trust information of any type or types. The web site, acting as a repository of trust information may be structured as an on-line directory of trust information for entities, similar to an online directory of telephone numbers. In techniques operating in a system such as the system of FIG. 1B, a user of the client device 112 may retrieve the trust information for an entity (e.g., entity 100' or entity 114A') prior to visiting the entity such that the user does not have to retrieve the trust information from the kiosk 102 or so that the entity does not have to provide the kiosk 102. Alternatively, the client device may retrieve the trust information while visiting the entity (e.g., shopping at a business) by accessing the server 116 through a wireless and/or wired network different than that of the wireless access point 104 (e.g., by accessing a WWAN network).

Server 116 may have a data store 120 comprising one or more pieces of trust information 122 (illustrated in FIG. 1B as "keys," but not so limited) for one or more entities. In some techniques operating in this system, a user may request from the server 116 an individual key for an individual entity, or may request a plurality of keys in any suitable group, such as entities in a certain geographic location or within a certain range of a certain geographic location, entities of a certain type, and/or entities associated with one another in a certain way (e.g., all businesses within a specified shopping mall).

The system of FIG. 1C shows another manner in which a client device 112 may retrieve trust information for one or more entities. In the system of FIG. 1C, a user 124 of the client device 112 may use a physical directory 126 to retrieve the trust information for one or more entities 100' and then manually enter the trust information into the client device 112 through any suitable user interface. The directory may be structured in any suitable manner, such as in a book format similar to a conventional telephone book (as illustrated in FIG. 1C) or as a sign listing trust information which may be displayed (e.g., mounted on a wall) within or near the entity (e.g., in a format similar to the floor map directories in shopping malls or as a sign at the entrance to a business). The directory 126

may provide trust information for one or more entities. In the case where the directory 126 provides information for multiple entities, the listed entities may be those in any suitable grouping, such as entities of a particular type or types, entities within a certain geographic area, or according to any other grouping. A user 124 may use the directory 126 to retrieve trust information for an entity prior to visiting the entity (for example, in the case where a directory 126 is structured like a telephone book), or may use the directory 126 while visiting the entity (for example, in the case where a directory 126 is a sign).

It should be appreciated that, in some implementations, multiple techniques for allowing client devices to retrieve trust information may be implemented in one system. For example, an entity may make its trust information available through a web service and/or a directory and may additionally provide one or more kiosks from which trust information may be retrieved, and may implement any other suitable technique as well, as the invention is not limited to implementing any single technique for providing or retrieving trust information alone or in combination with any other technique(s). It should also be appreciated that the invention is not limited to being performed with the illustrative techniques described above for retrieving trust information, as any suitable technique for retrieving trust information may be implemented in accordance with the principles described herein.

FIG. 2 shows an exemplary process 200 which implements some of the principles disclosed herein for passing content (e.g., information about products and/or services in the form of advertisements) between a wireless access point 104 of an entity 100 and a client device 112. It should be appreciated that the process 200 is merely illustrative and that the invention is not limited to implementing any particular process or processes for exchanging content between a wireless access point and a client device. As discussed above, it should be appreciated that, while process 200 is described in conjunction with advertisements, this type of content is merely illustrative as the invention is not limited to exchanging any particular type or types of content.

The process 200 begins in block 202, wherein an entity (or any person or device associated with an entity) specifies advertising information related to one or more services associated with the entity. The one or more services may be, as shown in FIG. 2, a commercial service, such as sale of a product through any service that may be performed by the entity. For example, if the entity is a restaurant, a commercial service provided by the entity may be serving food and the advertisement relating to the service may describe

the specials of the day served by the restaurant. As used herein the term "commercial service" is not limited to services provided by entities for profit. Commercial services may include announcements of events conducted by non-profit or governmental groups, such as free concerts.

In accordance with some techniques implementing the principles described herein, specifying advertising information in block 202 may comprise encoding in a data store associated with the wireless access point data describing one or more advertisements for the specified commercial service, while in other implementations specifying the commercial service may comprise selecting from a list of preconfigured products and/or services which product(s) and/or service(s) are to be the specified commercial service.

In block 204, the wireless access point transmits advertisement data relating to the specified advertisement information for the commercial service. In some implementations, the transmission sent by block 204 may be part of a control transmission sent by the wireless access point and may be, in accordance with some illustrative techniques for transmitting unrequested content, an announcement transmission such as a beacon broadcast periodically to all client devices within range of the wireless access point. The advertising data may be incorporated into the control transmission in any suitable manner. For example, in techniques which are implemented in an IEEE 802.11 wireless network, the advertisement data may be included in an information element of a beacon or probe response, though the invention is not limited to this exemplary technique and may incorporate content into control transmissions in any suitable manner.

In block 206, a client device retrieves trust information (e.g., a public key or PKI certificate) for the entity (i.e., for a wireless network comprising the wireless access point and/or for the wireless access point). This may be done in parallel with the acts 202 and 204, with the trust information being retrieved at the same time advertisement information is specified and transmitted, or may be done at any suitable time after the acts 202 and 204 have been completed. Retrieving trust information may be done in any suitable manner, such as by any of the illustrative techniques discussed above. The trust information may be retrieved from a kiosk, a server holding one or more pieces of trust information, a directory of trust information, and/or any other suitable "out of band" source of trust information.

In block 208, the client device 112 receives the control transmission of block 204 comprising the advertisement data and performs any suitable processing on the

transmission. In accordance with the principles disclosed herein, this processing comprises using the trust information in block 210 to confirm the identity of the wireless access point and/or the wireless network to which the wireless access point is connected. The processing of block 210 may be done in any suitable manner, including by any of the processes 300, 400, and 500 described in greater detail below.

In block 212, following the confirmation processing of block 210, the process 200 branches, depending on whether or not the wireless access point is the wireless access point from which the control transmission was received is the wireless access point from which the client device 112 expected to receive content (e.g., whether the wireless access point is authentic or fraudulent). If it is determined that the wireless access point is the expected wireless access point, then in block 214 the client device makes use of the content of the control message by, for example, presenting advertisement data to a user of the client device via a suitable user interface, and the process 200 ends. If, however, in block 212 the wireless access point is determined not to be the expected wireless access point, then in block 216 the wireless access point (and control messages transmitted by it) are ignored for a suitable period of time (e.g., minutes, days, until the client device exits the range of the wireless access point, until new trust information is obtained, forever, or any other suitable period of time).

It should be appreciated that process 200 is merely illustrative of techniques which implement some of the principles described herein, and that the invention is not limited to implementing a process such as process 200 or any particular process executing one or more acts of the process 200. Any suitable technique(s) for exchanging information about products and/or services between a wireless access point associated with an entity and a client device may be implemented in accordance with the principles described herein. For example, in alternative techniques, while FIG. 2 describes process 200 in terms of a commercial service being advertised by a commercial entity, embodiments of the invention may be implemented by entities which are not commercial entities, and as such the product(s) and/or service(s) associated with the entity may not be commercial services. Additionally, it should be appreciated that some alternative techniques may implement the acts shown in FIG. 2 in a different order. As an example, in some techniques operating in accordance with the principles described herein, a client device 112 may confirm the identity of a wireless access point 102 prior to receiving any control transmissions comprising advertisement data (or other content), such that the acts described above of

confirming the identity of a wireless access point and/or wireless network (i.e., acts 210 and 212) may be executed prior to the act 208.

As mentioned above in connection with process 200, confirming the identity of a wireless access point and/or wireless network (as in block 210 of process 200) may be done in any suitable manner. Discussed below in connection with FIGs. 3-5 are illustrative techniques for confirming the identity of wireless access points and/or wireless networks. It should be appreciated, however, that these techniques are merely exemplary of the types of techniques that may be implemented in accordance with the principles described herein, and that other techniques are possible.

FIG. 3 shows an exemplary process 300 by which the identity of a wireless access point may be confirmed. As above, while FIG. 3 is discussed in connection with advertisements and commercial entities, any suitable type or types of content may be used.

Process 300 begins in block 302, in which the client device retrieves trust information for one or more commercial entities. The trust information may comprise a public key and/or PKI certificate for the entity, and may be retrieved in any suitable manner, such as from a kiosk associated with the entity. In block 304, the client device detects that it is within range of a wireless access point for which it has trust information (e.g., by comparing an identifier for the detected wireless access point to identifiers for the trust information). In block 306, the client device transmits to the wireless access point a test control transmission which is encrypted using the trust information. The test control transmission may comprise any suitable information, and may include a challenge phrase and/or a nonce. Any suitable message may be used in the test control transmission (e.g., a random or pseudo-random bit string, unique text such as "Red trees are blue," a transmission time and/or transmission location, or any other suitable data). In some techniques operating according to the example of FIG. 3, the payload of the test control transmission may also comprise trust information for the client device 112, such as a public key/PKI certificate for the client device and/or a public key/PKI certificate for the user (collectively referred to below, for clarity, as the client trust information).

In block 308, the client device receives from the wireless access point a control transmission in response to the test control message. The response control transmission may comprise the contents of the test control transmission sent unencrypted or, in the implementations in which the test control message additionally included client trust information, the content of the response control message may be sent back encrypted

using the client trust information. If, upon receiving (and, in some techniques, decrypting) the response control transmission the client device determines that the contents match what was encrypted and transmitted (e.g., the contents of the test control transmission), then the client device may assume that the wireless access point holds the private key corresponding to the public key with which the contents of the test control transmission was encrypted and, therefore, that the wireless access point with which the client device is exchanging messages is the expected wireless access point.

In block 310, if the wireless access point is the expected wireless access point (e.g., if the wireless access point is authentic) then the client device may accept all future transmissions from the wireless access point as authentic, and use the contents of control messages freely (e.g., may display advertisements transmitted by the wireless access point to the user), and the process ends. If, however, in block 310 the wireless access point is determined not to be the expected wireless access point, then in block 314 the client device may ignore the wireless access point and control transmissions from the wireless access point for any suitable period of time.

In some implementations of techniques operating according to the example of FIG. 3, control messages comprising content (e.g., advertisement data) may not be transmitted encrypted, but rather are sent unencrypted. In some alternative implementations, following the authentication techniques of process 300, the wireless access point may, as an alternative to or in addition to broadcasting control messages, send to the client device control messages which are encrypted using the client trust information. In other embodiments, all or a portion of the control messages comprising content which are transmitted by the wireless access point are encrypted using the trust information for the wireless access point and the client device would decrypt each message using the trust information prior to using the contents (e.g., displaying the contents to a user).

In some techniques implementing the principles disclosed herein, confirmation of the identity of a wireless access point may rely on only the correct decryption of control messages for confirming the identity of a wireless access point and/or wireless network. FIG. 4 shows a process 400 which is illustrative of such techniques. As before, process 400 is discussed below in connection with advertisements for commercial entities, but techniques which may be implemented in accordance with some of the principles disclosed herein may exchange any suitable type or types of information as content of control messages.

Process 400 begins in block 402, in which the client device retrieves trust information for a commercial entity. The trust information may be retrieved in any suitable manner, such as by reading the trust information from a kiosk associated with the commercial entity. In block 404, the client detects that it is within range of a wireless access point for which it has trust information (e.g., by comparing an identifier for the detected wireless access point to identifiers for the trust information) and, in block 406, receives a control transmission (e.g., a beacon or a response to a probe request sent by the client device) from the wireless access point.

In block 408, the client device 112 processes the control transmission using the trust information retrieved in block 402 to confirm the identity of the wireless access point. Processing the control transmission may comprise using the trust information to decrypt the control transmission. If the control transmission can be correctly decrypted using the retrieved trust information, then the client device 112 may assume that the control transmissions were encrypted using a private key corresponding to the public key of the trust information, and thus that the wireless access point is the expected wireless access point and the transmission is authentic.

If, in block 410, it is determined that the transmission is authentic, then in block 412 the content of the control transmission may be used in any suitable manner, such as by extracting the advertisement and displaying it to a user, and the process ends. If, however, in block 410 the transmission is determined not to be authentic (i.e., the transmission cannot be confirmed to come from the expected wireless access point), then in block 414 the wireless access point is ignored for any suitable period of time, and the process ends without the contents being used.

FIG. 5 shows an alternative process 500 operating in accordance with some of the principles disclosed herein. Process 500 begins in block 502, in which the client device 112 retrieves trust information for a commercial entity. The trust information may be retrieved in any suitable manner, such as by retrieving the trust information from a server such as a server 116 that may, in some implementations of techniques operating according to the example of FIG. 5, implement a web service acting as a certificate authority and/or as a repository of trust information. The trust information retrieved in block 502 may be a single piece of trust information, or may be multiple pieces of trust information retrieved in any suitable grouping. In some implementations, the trust information may be retrieved in response to a user request, while in some implementations the client device 112 may be

adapted to retrieve, additionally or alternatively, the trust information automatically in response to any suitable stimulus. The stimulus may be a time or location (e.g., when the client device detects that it is near the location of an entity), a detection of a wireless access point associated with an entity, an indication received from the server 116 that previously-retrieved trust information has been added or changed, or any other suitable stimulus.

In block 504, the client device 112 detects that it is within range of a wireless access point for which it has trust information (e.g., by comparing an identifier for the detected wireless access point to identifiers for the trust information) and, in block 506, receives a control transmission (e.g., a beacon or a response to a probe request sent by the client device) from the wireless access point.

In block 508, the client device 112 processes the control transmission using the trust information retrieved in block 502 to confirm the identity of the wireless access point. Processing the control transmission may comprise using the trust information to decrypt the control transmission. If the control transmission may be correctly decrypted using the retrieved trust information, then the client device 112 may assume that the control transmissions were encrypted using a private key corresponding to the public key of the trust information, and thus that the wireless access point is the expected wireless access point and the transmission is authentic.

If, in block 510, it is determined that the transmission is authentic, then in block 512 the content of the control transmission may be used in any suitable manner, such as by extracting the advertisement and displaying it to a user, and the process ends. If, however, in block 510 the transmission is determined not to be authentic (i.e., the transmission cannot be confirmed to come from the expected wireless access point), then in block 514 the wireless access point is ignored for any suitable period of time, and the process ends without the contents being used.

It should be appreciated that the techniques described above in conjunction with FIGs. 3-5 are merely exemplary of the types of techniques that may implement some of the principles described herein for confirming the identity of wireless networks and/or wireless access points. It should be appreciated that the invention is not limited to implementing any particular one of these techniques, or limited to implementing any technique, as any suitable techniques may be implemented in accordance with the principles disclosed herein.

While the exemplary techniques described above focused on confirming the identity of a wireless access point and/or wireless network by decrypting control messages encrypted using trust information, the invention is not so limited. Techniques may be implemented that additionally or alternatively confirm the identity of wireless networks in other ways, including using environment information. For example, trust information for a wireless access point or wireless network may be an expected location for the wireless access point or wireless network and may be compared to location of the client device when within range of the wireless access point and/or to location information included in a control transmission from the wireless access point. In this manner, if the client device detects the wireless access point when it is not at the expected location, or if the location information in the control transmission is not the expected location information, then the detected wireless access point may be fraudulent. Location information which may be used may be any suitable location information, such as a street address, position within a building, latitude/longitude data, and/or any other suitable location information. Additionally or alternatively, environment information may comprise time information for the control transmission. Time information may be, for example, included in a control transmission describing a time at which the control transmission was first transmitted. A client device, upon receiving the control transmission, may compare the time information for the control transmission to trust information comprising a current time. The trust information may be used to determine if the broadcast time is within a reasonable difference from the current time. For example, if the difference between the broadcast time for a control transmission and the current time is greater than a certain amount of time (e.g., 10 seconds), the client device may determine that it is being subjected to a reply attack by a device rebroadcasting control transmissions, and determine that the detected wireless access point is fraudulent. Other embodiments may implement other techniques for confirming the identity of a wireless access point and/or wireless network, as the invention is not limited in this respect.

Discussed above are various techniques that may be used by client devices to implement some of the principles described herein. It should be appreciated, however, that in some systems implementing one or more of the principles described herein one or more elements of the wireless network to which a client device is connecting may execute techniques in accordance with these principles. FIG. 6 shows an exemplary process 600

that may be implemented by a wireless access point in accordance with some of these principles.

Process 600 begins in block 602, wherein the wireless access point retrieves local trust information from a data store. The local trust information may comprise any suitable trust information, such as a private key that may be used in a public key cryptography algorithm or any other suitable local trust information. In block 604, content is retrieved from data store 106 and encoded in a control transmission, and the control transmission is encrypted using the local trust information of block 602. The content encrypted in block 604 may be any suitable content, such as advertisement data, location data, data described one or more services offered by the wireless access point and/or the wireless network (e.g., printing services), or any other type of information. In block 606 the control transmission is then transmitted by the wireless access point. In some implementations, the control transmission may be transmitted as a beacon to all client devices within range of the wireless access point, while in alternative implementations the control transmission may be sent as a response to a probe request received by the wireless access point from a client device, or as any other suitable control transmission.

Techniques implementing one or more of the principles described herein may be implemented on any of numerous computer system configurations and are not limited to any particular type of configuration. FIGs. 7-8 show various computer systems in which embodiments of the invention may act, though others are possible. It should be appreciated that FIGs. 7-8 are intended to be neither a depiction of necessary components for a computing device to operate as a wireless access point or client device, nor a comprehensive depiction.

FIG. 7 shows an illustrative wireless access point 104. Wireless access point 104 comprises a processor 702, a network adapter 704, and computer-readable media 706. Network adapter 704 may be any suitable hardware and/or software to enable the wireless access point 104 to communicate with any other suitable computing device over any suitable computing network. The computing network may be any suitable wired and/or wireless communication medium or media for exchanging data between two or more computers, including the Internet. For example, the computing network may be, at least in part, a wireless network operating according to any suitable wireless networking protocol, such as IEEE 802.11, GSM, Bluetooth, WiMAX, UWB, and/or any other suitable protocol. In some embodiments of the invention, wireless access point 104 may comprise

two network adapters 704 to enable the wireless access point 104 to communicate with two different communication networks—for example, a wired computing network and a wireless computing network—and exchange data between the two. Computer-readable media 706 may be adapted to store data to be processed and/or instructions to be executed by processor 702. Processor 702 enables processing of data and execution of instructions. The data and instructions may be stored on the computer-readable media 706 and may, for example, enable communication between components of the wireless access point 104.

In accordance with some of the exemplary techniques described herein, data store 106 of FIGs. 1A, 1B, and 1C may be implemented as computer-readable media 706, and the data and instructions stored on computer-readable media 706 may comprise access point firmware 708, which may be software executed by the processor 702 instructing the wireless access point 104 to perform any suitable function, such as retrieving content (e.g., advertisement data 710 or other suitable content) from a data store for transmission, encoding the content in a control transmission, and generating a control transmission. The computer-readable media 706 may further store content such as advertisement data 710 (i.e., advertisement data 108). Advertisement data 710 may be any suitable type or types of data that may be transmitted by a wireless access point 104, including, for example, data describing text, images, audio, or video, or any combination thereof. The advertisement data 710 may be data describing a single advertisement for one or more services associated with an entity associated with the wireless access point 104, or may be data describing multiple advertisements for one or more services associated with an entity. In embodiments of the invention, the entity may be a commercial entity (e.g., a business) and the services may be commercial services. It should be appreciated, as discussed above, that advertisement data is merely illustrative of the type of content that may be transmitted by a wireless access point 104 in accordance with one or more of the principles described herein.

In accordance with some of the exemplary techniques described herein, computer-readable media 706 may further hold trust information 712 for the wireless access point 104 and/or a wireless network to which the wireless access point is connected. The trust information 712 may be any suitable trust information, such as a private key for the wireless access point 104 and/or wireless network to be used in a public key cryptography algorithm. It should be appreciated, however, that any suitable trust information may be used as trust information 712, including, for example, environment information, as a

private key is merely illustrative of the types of information that may be used as trust information in accordance with the principles described herein.

FIG. 8 shows an exemplary client device 112 which may be implemented as a client device in accordance with the principles described herein. As discussed above, any suitable computing device, mobile or immobile, may be used as a client device 112. Client device 110 may be a computing device designed for multiple purposes and for use by a user, such as a desktop personal computer, a laptop personal computer, a server, a personal digital assistant (PDA), a smart/mobile telephone, or any other suitable electronic device. Alternatively, client device 110 may be any computing device not intended for typical use by a user or intended for a single purpose or limited purposes, such as a server or a rack-mounted networking device.

Client device 112 comprises a processor 802, a network adapter 804, and computer-readable media 808. Network adapter 804 may be any suitable hardware and/or software to enable the client device 112 to communicate with any other suitable computing device over any suitable computing network. The computing network may be any suitable wired and/or wireless communication medium or media for exchanging data between two or more computers, including the Internet. For example, the computing network may be, at least in part, a wireless network operating according to any suitable wireless networking protocol, such as IEEE 802.11, GSM, Bluetooth, WiMAX, UWB, and/or any other suitable protocol. Network adapter 804 may further comprise an Application Programmer Interface (API) 806 to enable interaction between the network adapter 804 and applications executing on the client device 112. API 806 may provide executable functions to applications on the client device 112 such that the applications may request that network adapter 804 begin monitoring for transmissions from wireless access points, provide content from transmissions (e.g., advertisement data, location data, or any other suitable content), request additional information from the wireless access points, or any other suitable function. Computer-readable media 806 may be adapted to store data to be processed and/or instructions to be executed by processor 802. Processor 802 enables processing of data and execution of instructions. The data and instructions may be stored on the computer-readable media 806 and, for example, may enable communication between components of the client device 112.

In accordance with some embodiments of the invention, the data and instructions stored on computer-readable media 808 may comprise a user interface 810 by which the

content of control transmissions received by the network adapter 804 (e.g., advertisement data and/or additional information regarding advertised product(s) or service(s)) may be presented to a user. User interface 810 may present content in any suitable format. In some embodiments of a client device 112, the user interface 810 may be a component of an operating system or firmware of the client device 112, while in alternative embodiments of the invention the user interface 810 may be a standalone application, or a piece of an application such that the content may be displayed and used within the application.

In accordance with one or more of the principles described herein, computer-readable media 808 of the client device 112 may further comprise a data store of trust information 812. The trust information 812 may be one or more pieces of trust information for one or more wireless access points and/or wireless networks, and may comprise any suitable type or types of trust information. For example, as discussed above, the trust information may be public keys and/or PKI certificates for the wireless access points and/or wireless networks, and/or may be environment information such as time or location data for the wireless access points and/or wireless networks.

Computer-readable media 808 may further comprise a verification module 814 to test control messages received by the network adapter 804, using the trust information 812, to determine the authenticity of a wireless access point and/or wireless network. Verification module 814 may implement any suitable technique, including, but not limited to, any one or more of the exemplary techniques discussed above. In some implementations, the verification module 814 may be incorporated into an operating system of the client device 112, while in alternative implementations the verification module 814 may be implemented separate from the operating system, for example, as a stand-alone application executing on the client device 112 or in any other suitable manner.

The above-described embodiments of the present invention can be implemented in any of numerous ways. For example, the embodiments may be implemented using hardware, software or a combination thereof. When implemented in software, the software code can be executed on any suitable processor or collection of processors, whether provided in a single computer or distributed among multiple computers.

Further, it should be appreciated that a computer may be embodied in any of a number of forms, such as a rack-mounted computer, a desktop computer, a laptop computer, or a tablet computer. Additionally, a computer may be embedded in a device not generally regarded as a computer but with suitable processing capabilities, including a

Personal Digital Assistant (PDA), a smart phone or any other suitable portable or fixed electronic device.

Also, a computer may have one or more input and output devices. These devices can be used, among other things, to present a user interface. Examples of output devices that can be used to provide a user interface include printers or display screens for visual presentation of output and speakers or other sound generating devices for audible presentation of output. Examples of input devices that can be used for a user interface including keyboards, and pointing devices, such as mice, touch pads, and digitizing tables. As another example, a computer may receive input information through speech recognition or in other audible format.

Such computers may be interconnected by one or more networks in any suitable form, including as a local area network or a wide area network, such as an enterprise network or the Internet. Such networks may be based on any suitable technology and may operate according to any suitable protocol and may include wireless networks, wired networks or fiber optic networks.

Also, the various methods or methods outlined herein may be coded as software that is executable on one or more processors that employ any one of a variety of operating systems or platforms. Additionally, such software may be written using any of a number of suitable programming languages and/or conventional programming or scripting tools, and also may be compiled as executable machine language code or intermediate code that is executed on a framework or virtual machine.

In this respect, the invention may be embodied as a computer storage medium (or multiple computer readable media) (e.g., a computer memory, one or more floppy discs, compact discs, optical discs, magnetic tapes, flash memories, circuit configurations in Field Programmable Gate Arrays or other semiconductor devices, etc.) encoded with one or more programs that, when executed on one or more computers or other processors, perform methods that implement the various embodiments of the invention discussed above. The computer readable medium or media can be transportable, such that the program or programs stored thereon can be loaded onto one or more different computers or other processors to implement various aspects of the present invention as discussed above.

The terms “program” or “software” are used herein in a generic sense to refer to any type of computer code or set of computer-executable instructions that can be

employed to program a computer or other processor to implement various aspects of the present invention as discussed above. Additionally, it should be appreciated that according to one aspect of this embodiment, one or more computer programs that when executed perform methods of the present invention need not reside on a single computer or processor, but may be distributed in a modular fashion amongst a number of different computers or processors to implement various aspects of the present invention.

Computer-executable instructions may be in many forms, such as program modules, executed by one or more computers or other devices. Generally, program modules include routines, programs, objects, components, data structures, etc. that perform particular tasks or implement particular abstract data types. Typically the functionality of the program modules may be combined or distributed as desired in various embodiments.

Various aspects of the present invention may be used alone, in combination, or in a variety of arrangements not specifically discussed in the embodiments described in the foregoing and is therefore not limited in its application to the details and arrangement of components set forth in the foregoing description or illustrated in the drawings. For example, aspects described in one embodiment may be combined in any manner with aspects described in other embodiments.

Use of ordinal terms such as "first," "second," "third," etc., in the claims to modify a claim element does not by itself connote any priority, precedence, or order of one claim element over another or the temporal order in which acts of a method are performed, but are used merely as labels to distinguish one claim element having a certain name from another element having a same name (but for use of the ordinal term) to distinguish the claim elements.

Also, the phraseology and terminology used herein is for the purpose of description and should not be regarded as limiting. The use of "including," "comprising," or "having," "containing," "involving," and variations thereof herein, is meant to encompass the items listed thereafter and equivalents thereof as well as additional items.

Having thus described several aspects of at least one embodiment of this invention, it is to be appreciated that various alterations, modifications, and improvements will readily occur to those skilled in the art. Such alterations, modifications, and improvements are intended to be part of this disclosure, and are intended to be within the spirit and scope

of the invention. Accordingly, the foregoing description and drawings are by way of example only.

What is claimed is:

5

CLAIMS

1. A method of operating a client device (112) to display advertisement information (108) relating to a commercial service, the method comprising:

(A) obtaining (206) trust information for a wireless access point (104);

(B) verifying (210), based on the trust information, the authenticity of a control transmission from the wireless access point; and

(C) selectively displaying (214) to a user an advertisement for at least one commercial service contained within the control message based at least in part on the act of verifying.

2. The method of claim 1, wherein the act of verifying comprises transmitting (306) at least one message to the wireless access point.

3. The method of claim 2, wherein the commercial entity (100) is a mall or shopping center, and the trust information is one or more pieces of trust information for the mall and/or a business within the mall.

4. The method of claim 3, wherein the at least one message comprises device trust information for a device executing the method, and the act of verifying further comprises receiving (308) at least one response to the at least one message from the wireless access point and examining the at least one response using the device trust information.

5. The method of claim 1, wherein the act of verifying comprises decrypting at least a portion of the control transmission using the trust information.

6. The method of claim 1, wherein obtaining the trust information comprises obtaining the trust information from a device (102) implementing Near-Field Communication associated with the commercial entity.

7. The method of claim 1, wherein obtaining the trust information comprises obtaining the trust information from a web service (116) acting as a repository of trust information.

8. The method of claim 1, wherein the act of obtaining the trust information comprises a user (124) inputting the trust information after obtaining it from a directory (126).

9. The method of claim 1, wherein the trust information is a public key of a public key cryptography algorithm implemented by the wireless access point.

10. The method of claim 1, wherein the control transmission comprises environment information for the control transmission,

the method further comprises verifying the environment information, and

selectively displaying the advertisement to the user is based at least in part on a result of verifying the environment information.

11. The method of claim 11, wherein the environment information is a location for the wireless access point transmitting the control transmission and/or a time the control transmission was transmitted.

12. At least one computer-readable medium encoded with computer-executable instructions which, when executed, cause a computer to execute a method for confirming authenticity of a control transmission from a wireless access point (104) associated with an entity (100), the method comprising:

(A) obtaining (206) trust information for the entity (100);

(B) verifying (210), using the trust information, the authenticity of a control transmission from the wireless access point; and

(C) selectively using (214) contents of the control transmission based at least in part on the act of verifying.

13. The at least one computer-readable medium of claim 12, wherein the trust information is a public key for a public key encryption algorithm used to encrypt at least a portion of the control transmission.

14. The at least one computer-readable medium of claim 12, wherein the content is location data for the wireless access point and using the contents comprises determining a current location for a client device.

15. The at least one computer-readable medium of claim 12, wherein obtaining the trust information comprises obtaining the trust information from a kiosk (102) associated with the entity (100).

16. The at least one computer-readable medium of claim 12, wherein the control transmission comprises environment information for the control transmission,

the method further comprises verifying the environment information, and

selectively using the contents is based at least in part on a result of verifying the environment information.

17. An apparatus (104) for transmitting control messages in a wireless network, the apparatus comprising:

at least one data store (706) storing trust information (712) and contents (710);

at least one processor (702) adapted to construct a control transmission comprising the contents and to encrypt at least a portion of the control transmission using the trust information; and

a communication circuit (704) to transmit the control transmission.

18. The apparatus of claim 17, wherein the trust information is a private key of a public key encryption algorithm.

19. The apparatus of claim 17, wherein the communication circuit is adapted to transmit a responsive test control message constructed by the at least one processor in response to a test control message received from a client device, the test control message comprising at least one nonce.

20. The apparatus of claim 17, wherein the content is location data describing a location of the apparatus.

5

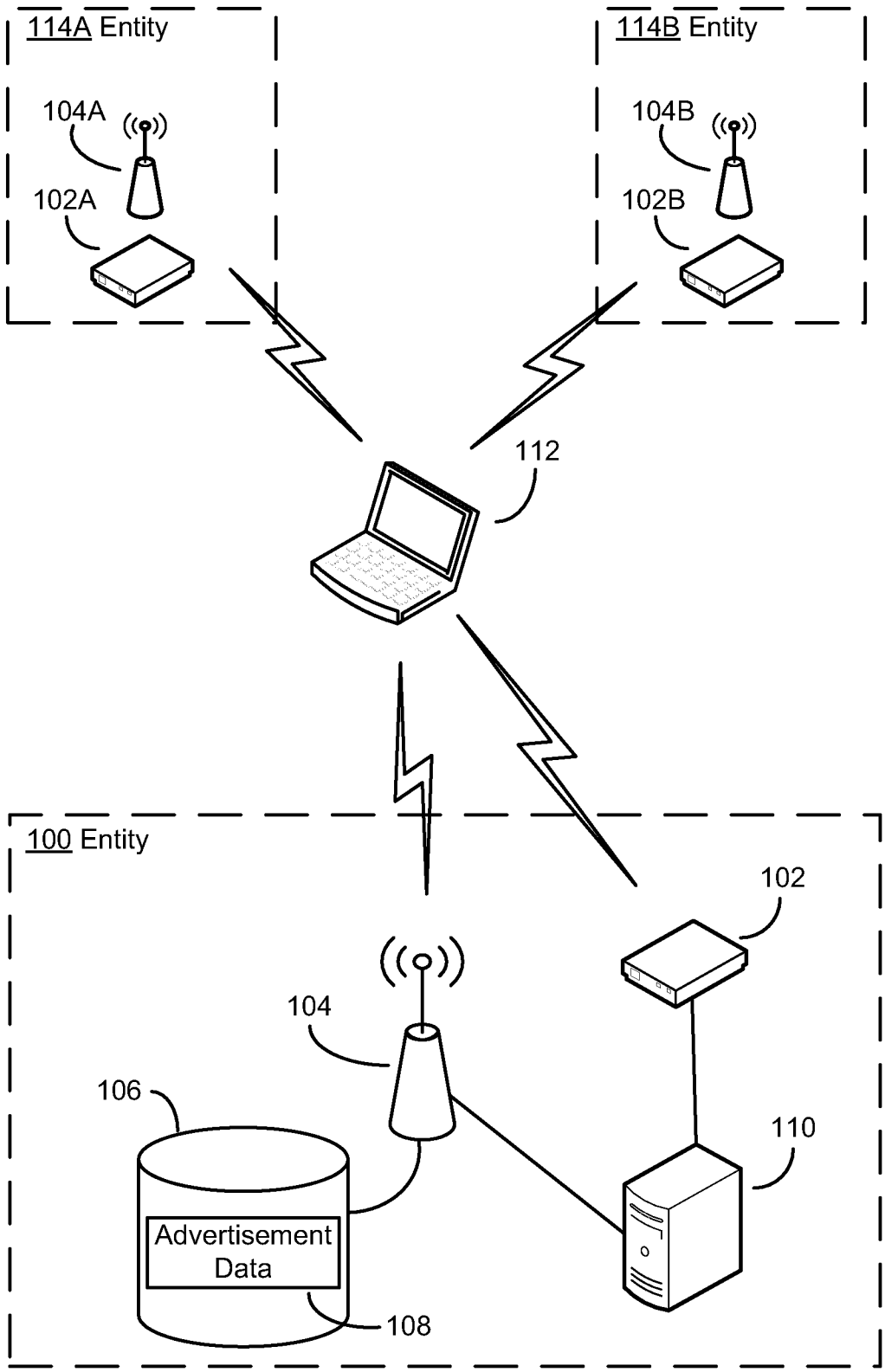
114A Entity
104A
102A
114B Entity
104B
102B
112
100 Entity
102
104
106
110
Advertisement Data
108

FIG. 1A

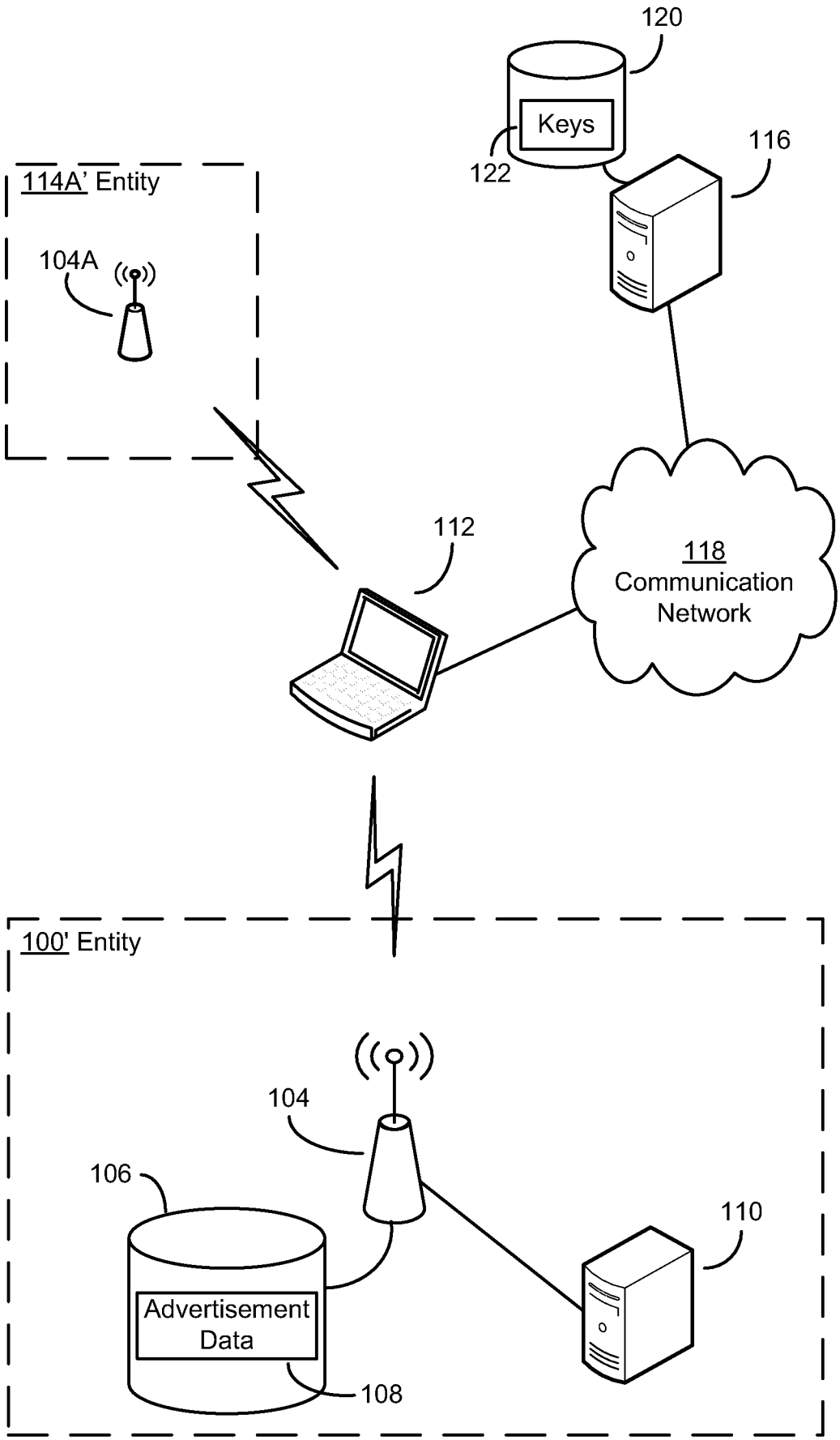
120
Keys
122
116
114A' Entity
104A
112
118
Communication
Network
100' Entity
104
106
110
Advertisement
Data
108

FIG. 1B

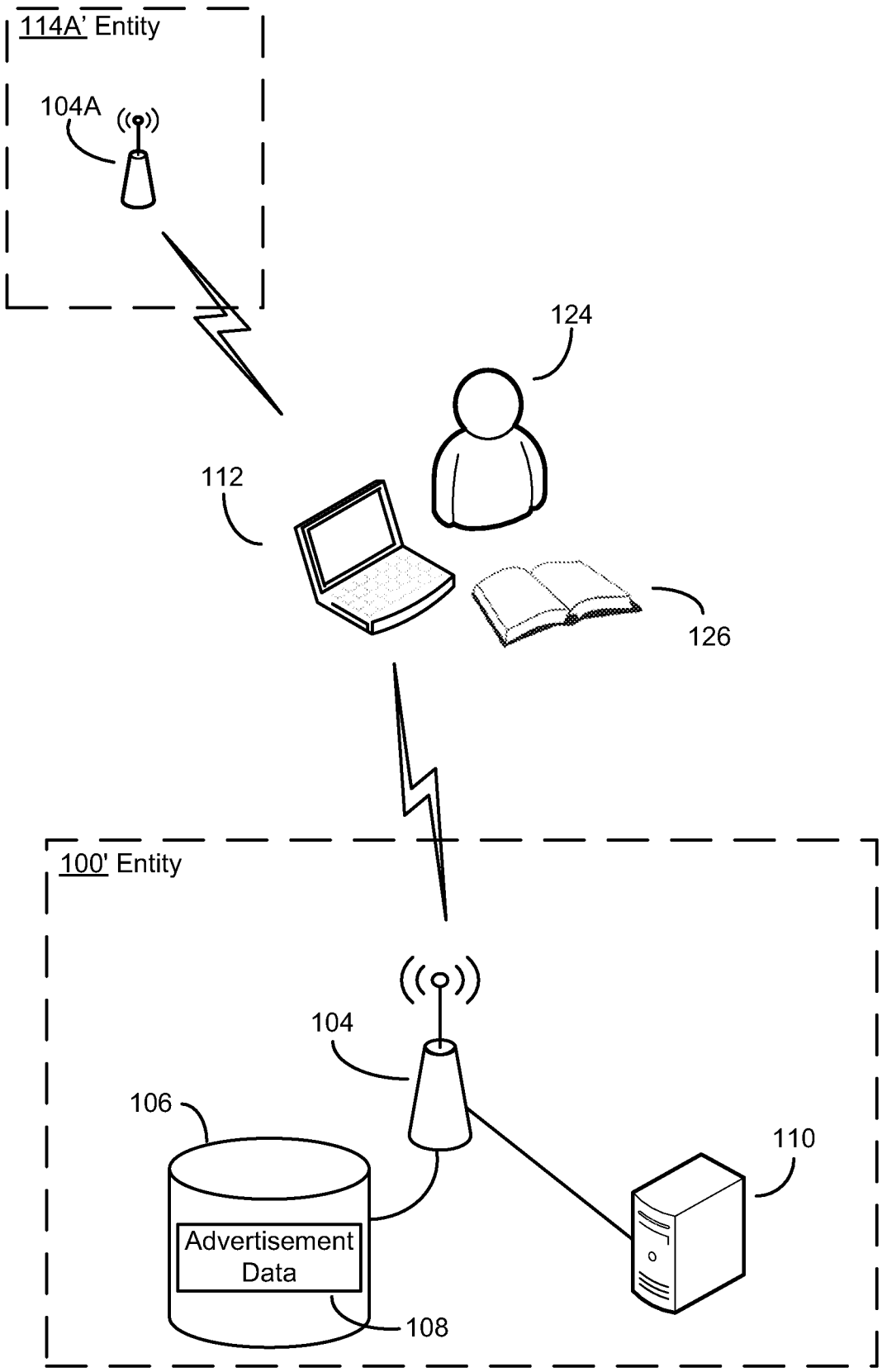
114A' Entity
104A
124
112
126
100' Entity
104
106
110
Advertisement Data
108

FIG. 1C

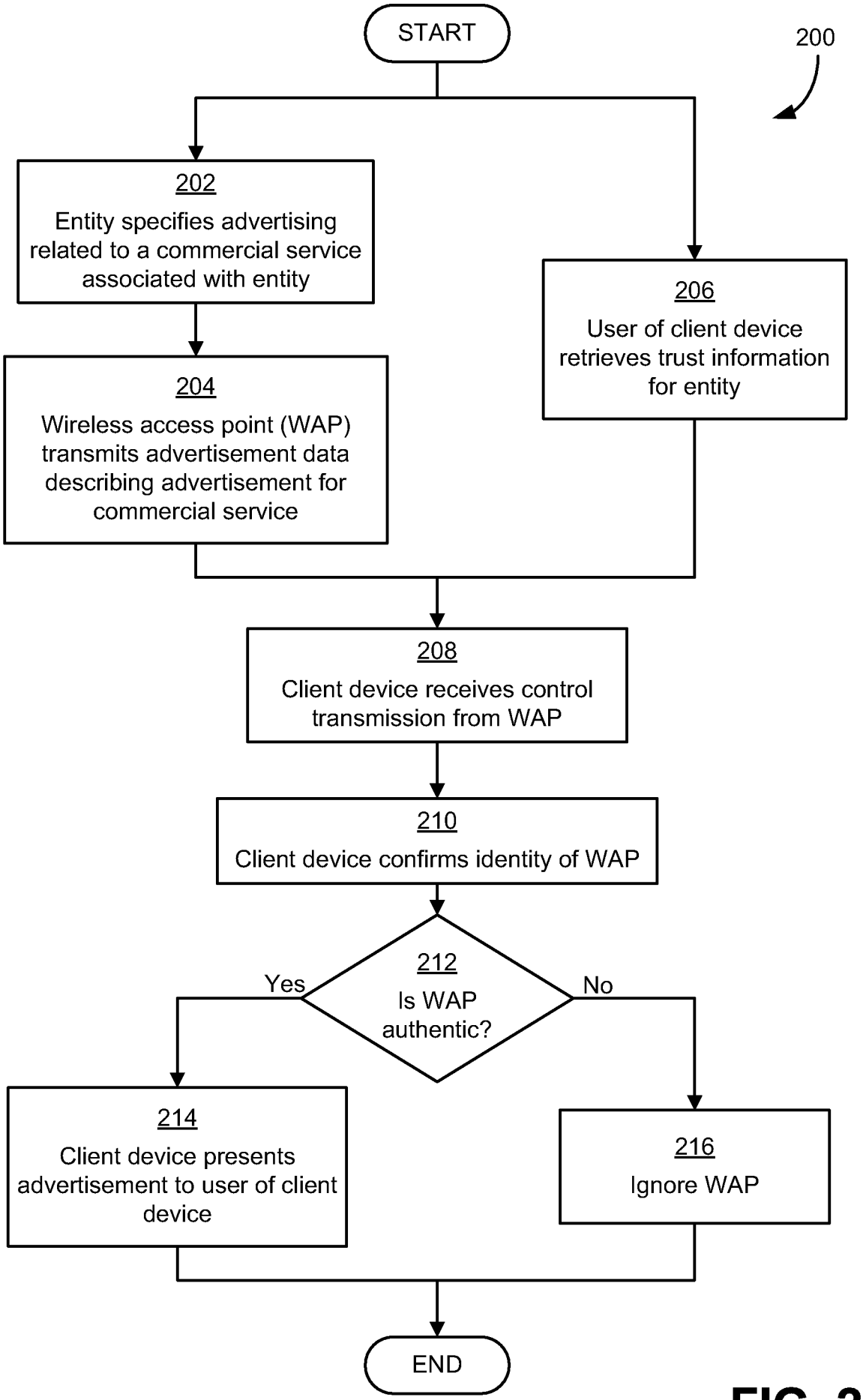
START
200
202
Entity specifies advertising related to a commercial service associated with entity
204
Wireless access point (WAP) transmits advertisement data describing advertisement for commercial service
206
User of client device retrieves trust information for entity
208
Client device receives control transmission from WAP
210
Client device confirms identity of WAP
212
Is WAP authentic?
Yes
No
214
Client device presents advertisement to user of client device
216
Ignore WAP
END

FIG. 2

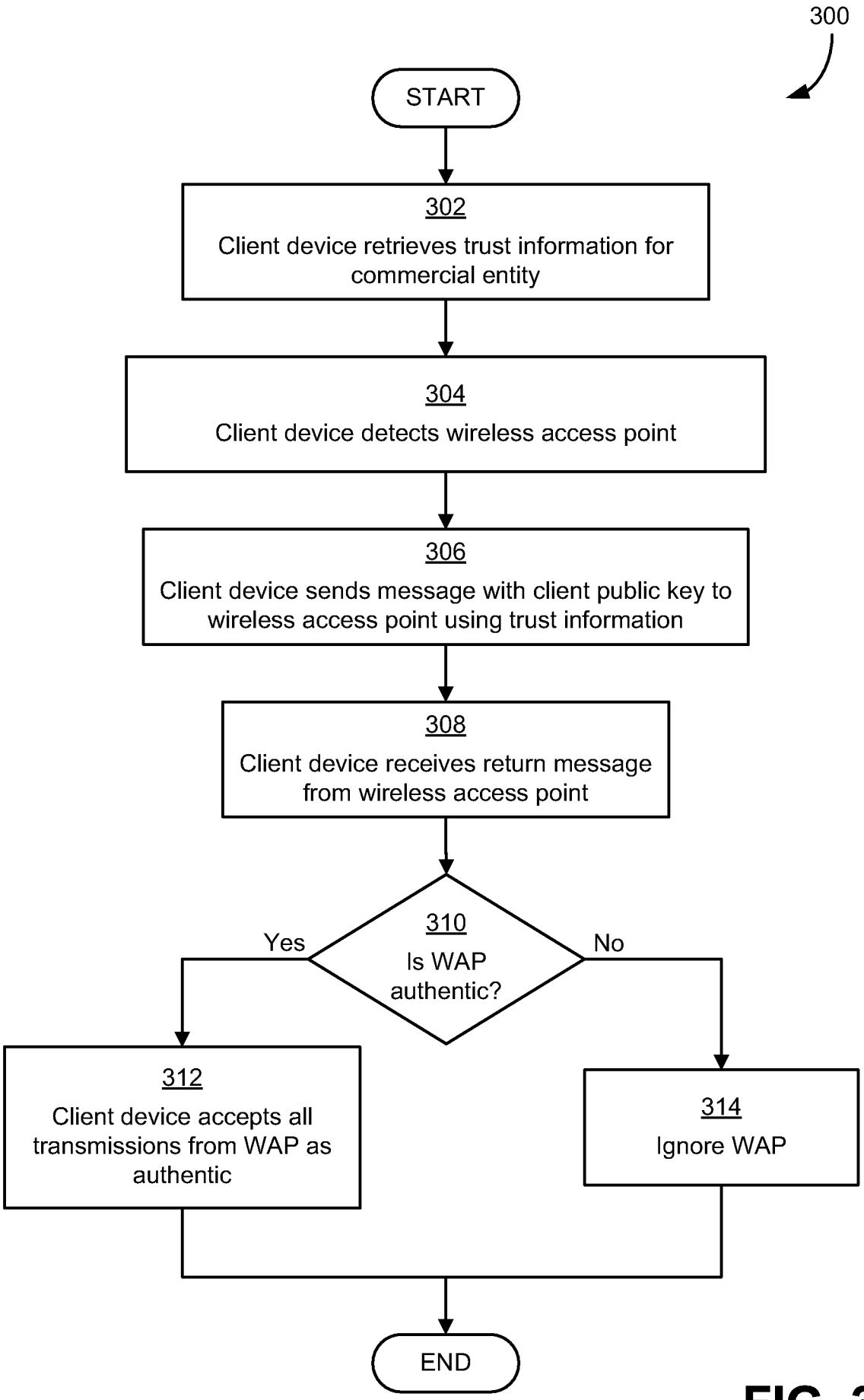
300
START
302
Client device retrieves trust information for commercial entity
304
Client device detects wireless access point
306
Client device sends message with client public key to wireless access point using trust information
308
Client device receives return message from wireless access point
310
Is WAP authentic?
Yes
No
312
Client device accepts all transmissions from WAP as authentic
314
Ignore WAP
END

FIG. 3

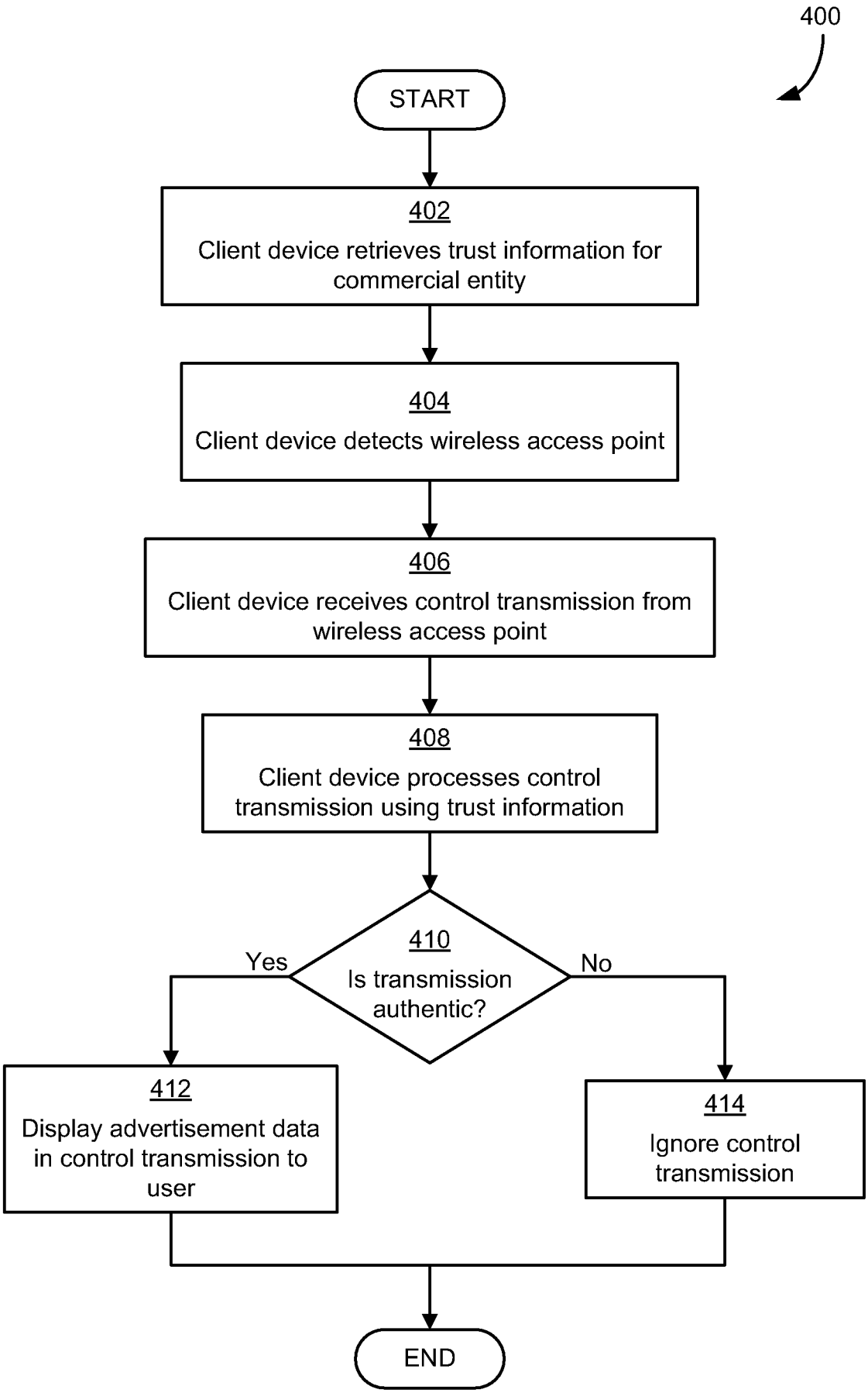
400
START
402
Client device retrieves trust information for commercial entity
404
Client device detects wireless access point
406
Client device receives control transmission from wireless access point
408
Client device processes control transmission using trust information
410
Is transmission authentic?
Yes
No
412
Display advertisement data in control transmission to user
414
Ignore control transmission
END

FIG. 4

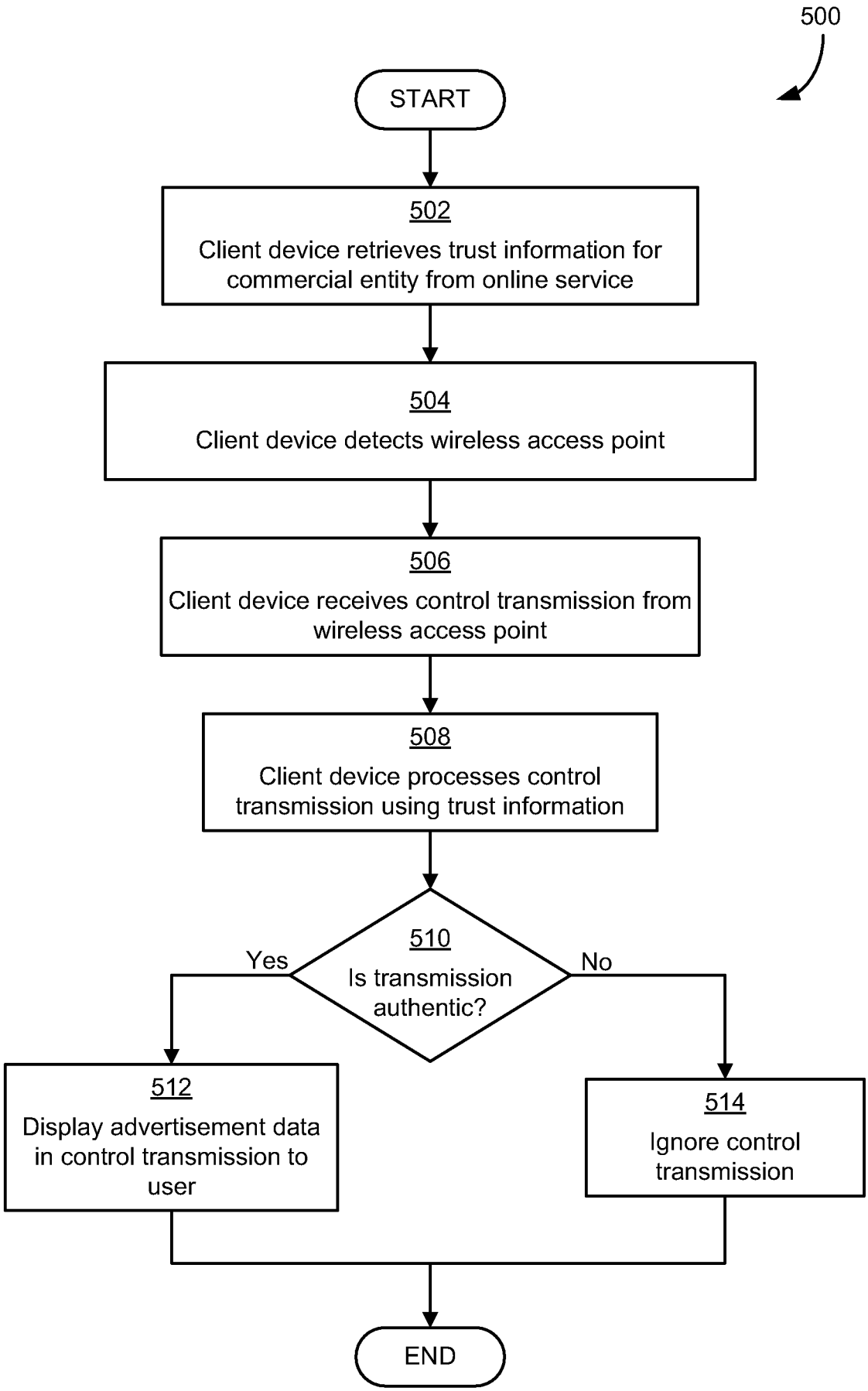
500
START
502
Client device retrieves trust information for commercial entity from online service
504
Client device detects wireless access point
506
Client device receives control transmission from wireless access point
508
Client device processes control transmission using trust information
510
Is transmission authentic?
Yes
No
512
Display advertisement data in control transmission to user
514
Ignore control transmission
END

FIG. 5

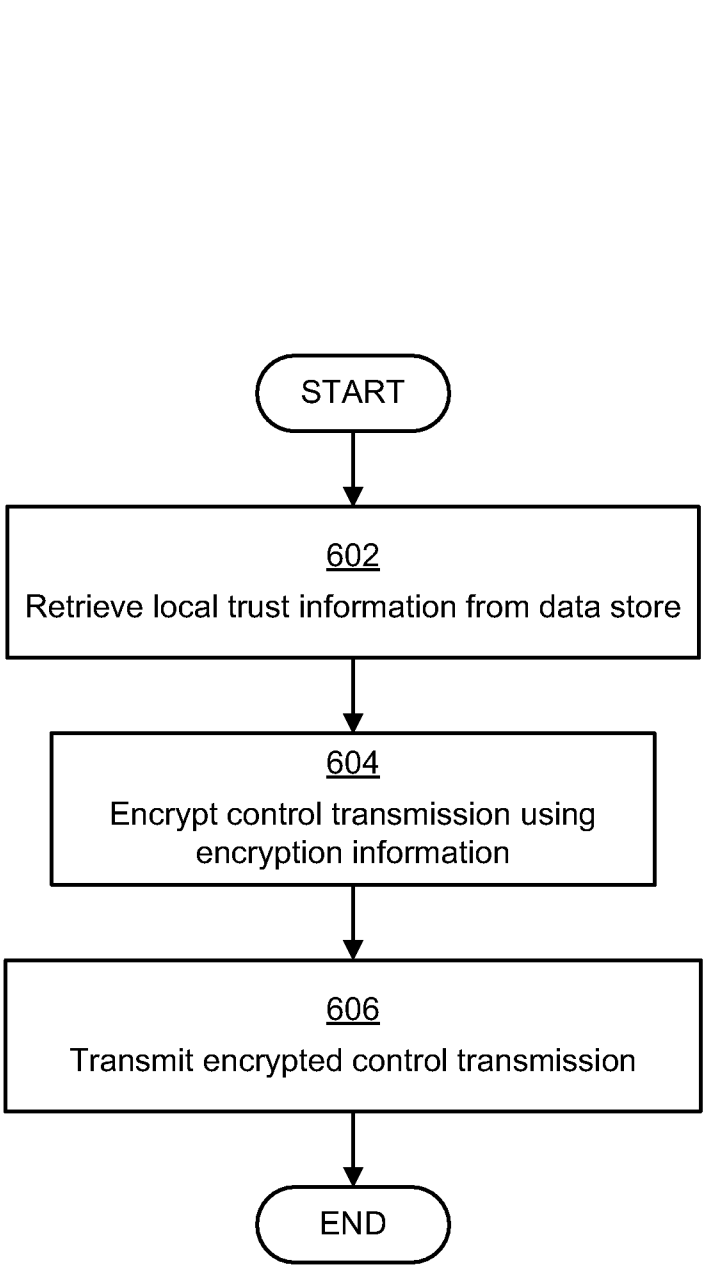
600
START
602
Retrieve local trust information from data store
604
Encrypt control transmission using encryption information
606
Transmit encrypted control transmission
END

FIG. 6

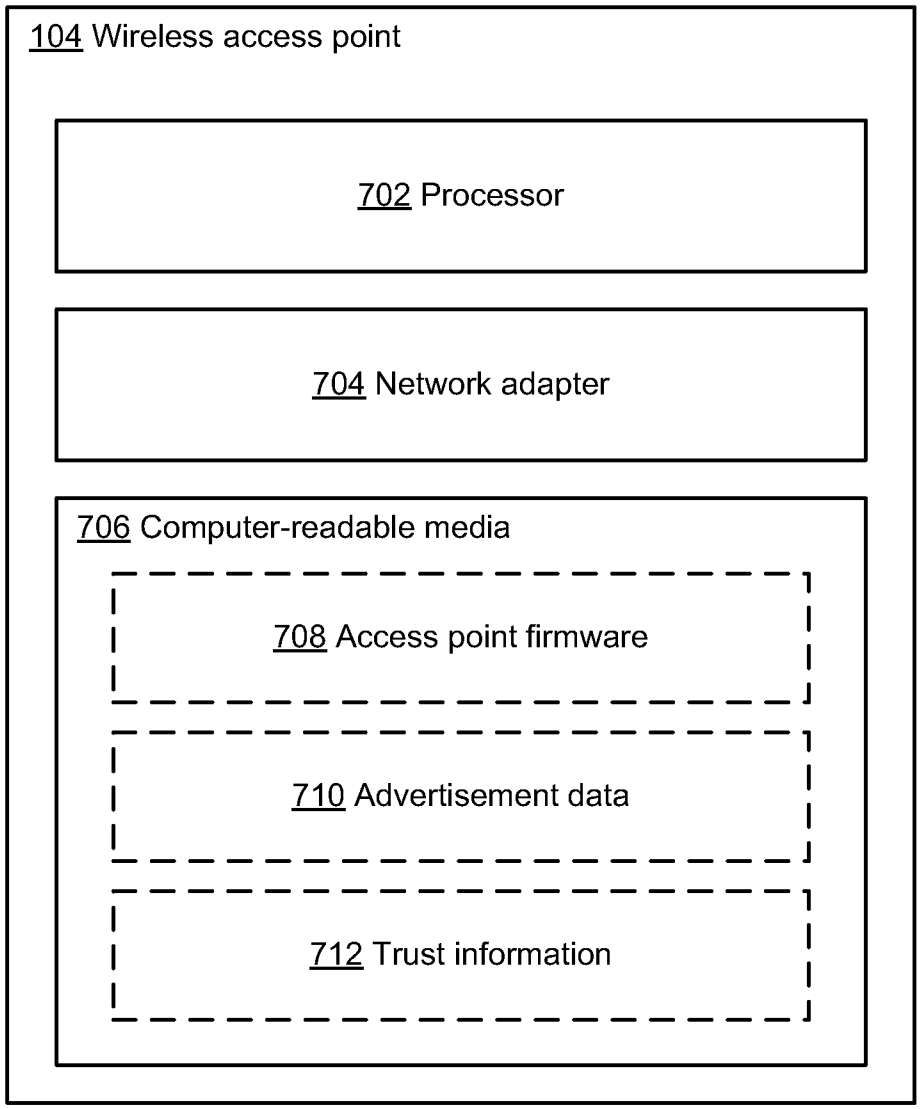
104 Wireless access point
702 Processor
704 Network adapter
706 Computer-readable media
708 Access point firmware
710 Advertisement data
712 Trust information

FIG. 7

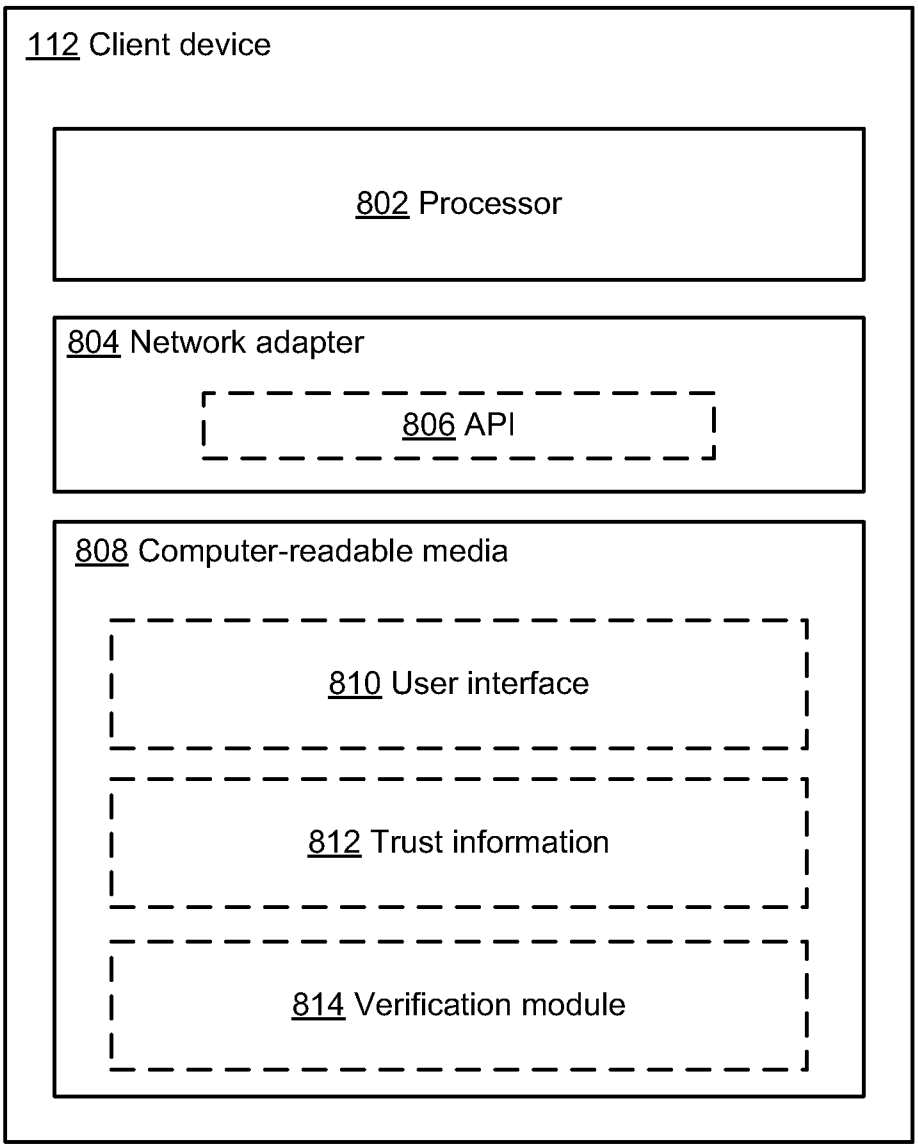
112 Client device
802 Processor
804 Network adapter
806 API
808 Computer-readable media
810 User interface
812 Trust information
814 Verification module

FIG. 8

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
322624.02 WO		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/US2009/031451	**20 JANUARY 2009 (20.01.2009)**	22 FEBRUARY 2008 (22.02.2008)

Applicant

MICROSOFT CORPORATION

This International search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of **3** sheets.

☐ It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**
   a. With regard to the **language**, the international search was carried out on the basis of :
      ☒ the international application in the language in which it was filed
      ☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. ☐ This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6*bis*(a)).
   c. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.
2. ☐ **Certain claims were found unsearchable** (See Box No. II)
3. ☐ **Unity of invention is lacking** (See Box No. III)
4. With regard to the **title,**
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established by this Authority to read as follows:
5. With regard to the **abstract,**
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.
6. With regard to the drawings,
   a. the figure of the **drawings** to be published with the abstract is Figure No. **1**
      ☒ as suggested by the applicant.
      ☐ as selected by this Authority, because the applicant failed to suggest a figure.
      ☐ as selected by this Authority, because this figure better characterizes the invention.
   b. ☐ none of the figure is to be published with the abstract.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2009/031451

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(2006.01)i, G06F 21/20(2006.01)i, G06Q 30/00(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04L, H04W, G06F, G06Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

KOREAN UTILITY MODELS AND APPLICATIONS FOR UTILITY MODELS SINCE 1975
JAPANESE UTILITY MODELS AND APPLICATIONS FOR UTILITY MODELS SINCE 1975

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKIPASS (KIPO internal) & keywords : authenticate, advertise

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2005-0083929 A (JUBA M. SALO et al.) 21 April 2005 See abstract; paragraphs 6, 7, 13, 15, 48-53; claims 1-3, 10-12 and figures 1, 6.	1-20
A	KR 10-2000-0017730 A (RANG HA LEE et al.) 06 April 2000 See abstract; claims 1, 4, 5 and figures 1, 2.	1-20
A	KR 10-2006-0002649 A (PANTECH & CURITEL COMMUNICATIONS, INC.) 09 January 2006 See abstract; claim 1 and figures 1, 2.	1-20
A	EP 1760654 A1 (PALO ALTO RESEARCH CENTER INCORPORATED) 07 March 2007 See abstract; paragraphs 16, 27, 32; claim 1 and figures 5, 6, 8.	1-20

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 JUNE 2009 (26.06.2009)	**29 JUNE 2009 (29.06.2009)**

Name and mailing address of the ISA/KR
Korean Intellectual Property Office
Government Complex-Daejeon, 139 Seonsa-ro, Seo-gu, Daejeon 302-701, Republic of Korea
Facsimile No. 82-42-472-7140

Authorized officer
YANG, Jeong Rok
Telephone No. 82-42-481-5709

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2009/031451

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2005-0083929 A1	21.04.2005	PI 0415982 A	23.01.2007
		CA 2542933 A1	28.04.2005
		CN 1883180 A	20.12.2006
		EP 1676416 A2	05.07.2006
		JP 2007-509565 A	12.04.2007
		KR 10-2006-0092264 A	22.08.2006
		TW 253824 B	21.04.2006
		WO 2005-039146 A2	28.04.2005
KR 10-2000-0017730 A	06.04.2000	None	
KR 10-2006-0002649 A	09.01.2006	None	
EP 1760654 A1	07.03.2007	US 2007-0061057 A1	15.03.2007
		JP 2007-068164 A	15.03.2007