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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 September 2010 (23.09.2010)

PCT

(10) International Publication Number
WO 2010/106537 A2

(51) International Patent Classification:
G08B 25/10 (2006.01) *G06Q 30/00* (2006.01)

(21) International Application Number:
PCT/IL2010/000215

(22) International Filing Date:
15 March 2010 (15.03.2010)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

61/160,319	15 March 2009 (15.03.2009)	US
61/163,120	25 March 2009 (25.03.2009)	US

(71) Applicant *(for all designated States except US)*: **AUTHIX TECNOLOGIES SRL.** [IT/IT]; Corso Castelfidardo 30/A, I-10129 Torino (IT).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **TSURIA, Yossef** [IL/IL]; 14 Rabenu Polity Street, 93390 Jerusalem (IL). **MAYTAL, Benjamin** [IL/IL]; 6 Tzabar Street, 90805 Mevasseret Zion (IL). **ROSNER, Amit** [IL/IL]; 46 Golda Meir Street, 56207 Yahud (IL).

(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, CL, 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, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

(54) **Title**: REMOTE PRODUCT AUTHENTICATION

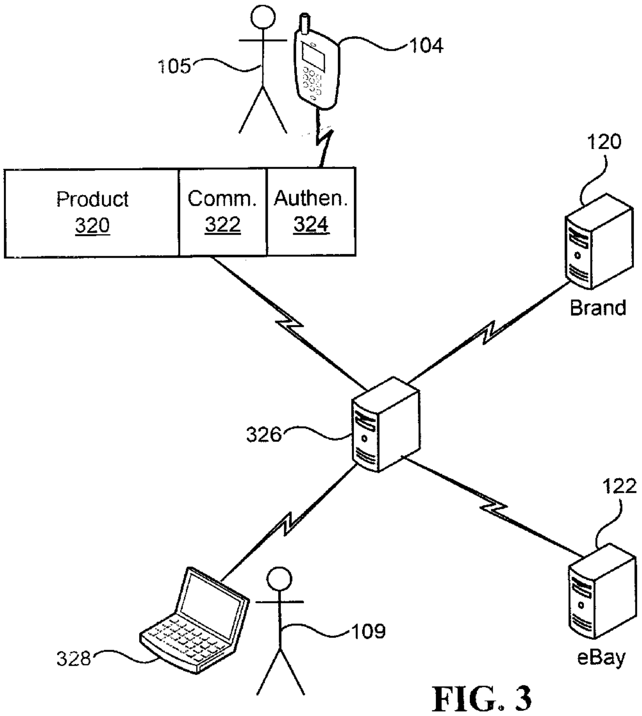

FIG. 3

(57) **Abstract**: Methods of enabling a buyer to authenticate a product offered by a seller, in which the buyer notifies the seller of a desire to authenticate the product, and the seller then requests authentication of the product from a server database containing authentication data regarding said product. The server is programmed to provide the result of the product authentication only to said second party. Alternatively, the server can provide the seller with an authentication certificate which the seller can supply to the buyer. Authentication tags, such as for use in these systems, are also described where an antenna tuned to receive mobile phone transmission is connected to a capacitor and the capacitor is connected to active logic via a voltage regulator. Other embodiments disclose such tags in which a battery is connected to active logic through the control of a circuitry detecting mobile phone transmission.

REMOTE PRODUCT AUTHENTICATION

FIELD OF THE INVENTION

The present invention relates to the field of product authentication, especially methods and systems for authenticating products available remotely from the interested buyer, such as over the Internet or phone, and also for tags attached to the products and communicating with an external authentication application.

BACKGROUND OF THE INVENTION

Published PCT Application WO 2008/065649 and US Application No. 12/276,620, both incorporated by reference herein in their entireties, disclose various authentication tags enabling wireless authentication, such as a challenge-response authentication process. Such authentication tags may comprise one or more of the following components: a memory for the authentication software, such as random access memory (RAM); an authentication block, such as a challenge-response authentication block or any other symmetric or asymmetric authentication logic; a memory for storing the authentication identification number, such as EEPROM; a microcontroller; a short range communication device, such as Bluetooth communication; and a power supply. Optionally, the authentication tag is coupled to a product to be authenticated.

In order to authenticate the product, a communication device, such as a mobile phone, a Personal Digital Assistant (PDA), or a computer, is placed close to the product to be authenticated. The communication device communicates with the tag and, optionally, authenticates the tag utilizing an authentication server.

However, such prior art authentication systems are generally effective only for situations where the buyer has direct access to the product being sold, such as in a shop. In such a situation the purchaser can make contact with the product identification tag using his/her own authentication application, and for instance, conduct an authentication procedure with a remote server to ascertain that the product is genuine. However, there exists a problem for the authentication of products sold over the Internet or over the phone, where the buyer has to rely on the credibility of the seller, since he has no access to the product until the buyer receives the shipment from the seller, at which point the sale has been consummated. Retraction of the transaction then involves arguments, proofs, communication and potential unpleasantness. Some web sale sites, such as eBay or other such Internet online store, do however have some level of responsibility for the authenticity of products sold thereon, since sellers can be rated on the basis of feedback received from the buyers, and sellers purveying fake products will soon be barred from the site. However, there still exists a need for a better system enabling a web buyer to verify the authenticity of a produ:t he/she is purchasing, before the item is shipped to him/her, without the need for reliance on the credibility of the seller. Future references in this disclosure to persons, will be made in the masculine only, even though it is to be understood that both genders are equally intended.

Such systems are dependent on authentication tags attached to the products to be authenticated. US Patent application 12/276,473 describes a product electronic tag which can interface with a mobile phone using Bluetooth communication and is charged through the mobile phone transmitted energy. According to this concept, the user who wishes to authenticate a product will hold the mobile phone close to the product he wishes to verify, in order to power the tag so that it can communicate with the authenticating system by means of a short range link, such as Bluetooth. The tag described in that application suffers from several problems which may prevent it from achieving the target of a passive tag communicating via Bluetooth.

Firstly, the power received by the antenna may charge the capacitor to voltages which are sufficiently high to damage the tag VLSI devices.

The second problem is that VLSI components have a narrow range of operation, typically only about 0.2v, and the capacitor is continuously charging and discharging. In order to maintain a reasonably constant output, a very large capacitor would be required.

A third problem is primarily commercial, rather than technical. The tags are meant for anti-counterfeit product protec:on. It is very likely they will be put in the product package. This presents a risk – the seller who wishes to sell fake products may offer an incentive to the customer to return to him the product package, and he may use it to wrap a fake product.

There is therefore a requirement for an effective small, low cost tag which overcomes these problems.

The disclosures of each of the publications mentioned in this section and in other sections of the specification are hereby incorporated by reference, each in its entirety.

SUMMARY OF THE INVENTION

Systems described in the present disclosure, provide a buyer with novel methods for ascertaining the authenticity of a product ordered over a network where the buyer does not have access to the product before it is dispatched by the seller. The system depends on a flow of authentication information in which the party requesting the authentication from a remote server is not the party that performs the authentication operation. In one exemplary implementation, when the buyer wishes to make a purchase, he requests of the seller to implement an authentication procedure of the product, in whatever manner is predetermined for such sales or products, and the system is designed such that the authentication information is returned to the buyer, rather than to the seller who requested it. By this means, the authentication information is safeguarded from being tampered with by the seller, such that the buyer can be assured that he will receive a bone fide authentic product, even before closing the transaction and paying for the product.

As an extension of this scheme, the seller may be allowed to receive authentication information from the server, on condition that it is in the form of an authentication certificate which cannot be forged, and which is forwarded to the buyer such that it can be confirmed by the buyer when he receives the product and the authentication certificate.

There are a number of alternative ways in which such a remote authentication scheme can be implemented, as follows.

In some embodiments, the seller places his authentication device close to a product coupled to a tag to be queried. Optionally, the authentication device charges the tag coupled to the product to be authenticated. Optionally, the authentication device is one or more of the following: a mobile phone, an electronic device comprising Bluetooth, or a PC/PDA configured to communicate with the authentication server and the tag without the assistance of a mobile phone.

In one embodiment, the seller operates his authentication device in an auto-receive mode enabling him to leave his authentication device close to the product to be queried with the authentication application running. In this case, the buyer may authenticate the product without the seller's assistance. The buyer may authenticate the product using an appropriate authentication software, which may run on the buyer's mobile phone or on any other device having appropriate communication means.

In some embodiments, after the seller authenticates the product, the authentication result may be forwarded to one or more of: the buyer, seller, brand server, or trade website. In those cases where the seller is provided with authentication data, it should be in the form of a reliable authentication certificate, since otherwise the seller could send a fake article to the buyer, yet supply bone fide authentication with it. While it is true that the seller can authenticate a good product and ship another, the buyer will be able to perform authentication again – and the buyer can report such a seller to the website.

In one embodiment, the buyer receives the authentication answer and verifies that the product is genuine by communicating with a predefined server, such as the manufacturer's server, an authentication server, a website server, etc.

In one embodiment, a predefined server receives the authentication answer and verifies that the product is genuine. Optionally, and in some cases, against payment, the predefined server may notify the buyer whether or not the product is genuine. Optionally, the predefined server sends other information that is related to the product such as production date, features of the product, etc.

In one embodiment, a predefined server receives the authentication answer, verifies that the product is genuine, notifies the buyer whether or not the product is genuine, and provides the buyer with data that will enable the buyer to verify that he received the specific product that was authenticated.

Examples of the data provided by the server include: the authentication result, a unique product serial number, a unique authentication identification information that enables the authentication server to identify the specific product, and a unique authentication transaction identification that enable the authentication server to identify the transaction and from the transaction data to locate the product data.

When the buyer authenticates a product (before buying it) he receives from the authentication system the ID of the product or other product identification means. When the buyer receives the product, he can compare the product ID received from the authentication system with the ID of the product received from the seller. If the ID's match, the buyer knows that he received the promised product.

In one embodiment, the seller forwards an authentication certificate to the buyer. The embodiment comprises the following steps:

(i) A seller authenticates the product with an authentication server;

(ii) The seller receives a certificate from the authentication server;

(iii) The seller forwards the certificate to a potential buyer; and

(iv) The Buyer receives and authenticates the product using the authentication certificate.

Optionally, in addition to receiving the authentication certificate, the buyer also authenticates the product similarly to the way in which the seller authenticated the product, for example, using a mobile phone and/or using short range communication such as Bluetooth. The authentication server authenticates the product and verifies whether the product is genuine. Alternatively, the authentication server authenticates the product and verifies that the product is the one previously authenticated by the seller.

In one embodiment, the authentication server stores the authentication certificate. The embodiment comprises the following steps:

(i) The seller authenticates a product using an authentication server;

(ii) The authentication server stores the authentication result, which may be alternatively referred to as the authentication certificate;

(iii) The buyer receives from the seller data that enables the buyer to receive the product's certificate from the authentication server. Optionally, the data received by the buyer from the seller is coupled to the product, such as the product serial number. Optionally, the data received by the buyer from the seller is a code. Optionally, the data received by the buyer from the seller is created by the authentication server for the specific product.

(iv) The Buyer sends the information received from the seller to the authentication server; and

(v) The Buyer receives confirmation and authenticates the product.

In one embodiment, the following method steps are performed to authenticate a product on a website:

(i) A seller offers one or more of his products over a trade website, such as eBay or any other Internet online store;

(ii) Optionally, a potential buyer indicates he wishes to verify that the product is genuine;

(iii) Before the seller ships the product to the buyer, the seller authenticates the product to be shipped utilizing an authentication server; and

(iv) Then the authentication server notifies at least one of the seller, buyer, or the website of the authentication result.

In addition, according to further aspects of the invention described in the present application, there are provided new electronic tags, such as for use in the above desribed product authentication, by means of communication with an authentication application running on a mobile phone held near the tag. According to one exemplary implementation, the tag is powered by an on-board battery, which, because of its small dimensions, is unable to supply the continuous current required by the processing circuits on the tag. A capacitor is installed on the tag in order to store charge provided by current from the battery. In this manner, the capacitor behaves like a current buffer between the battery and the processing circuits which need to be powered. In order to ensure that the correct voltage is applied to the processing circuits, an electronic switch is located between the capacitor output and the processing circuits, and is only closed to allow supply of current from the capacitor, when the voltage is sufficient to power the processing circuits. The switch may be activated by means of a voltage sensing circuit detecting the voltage on the capacitor. A voltage regulator may be used between the capacitor and the processing circuits, in order to stabilize the voltage applied to the processing circuits.

According to another exemplary implementation, in order to conserve the limited energy stored in the battery, the battery is only connected to the storage capacitor of the tag when the tag is in the presence of a mobile phone transmission of sufficient strength, since it is only when such a field is present that the tag needs to be operable. This is achieved by means of an electronically operated switch located between the battery and the capacitor.

The switch is activated by means of a mobile phone transmission detection circuit, which opens or close since they switch according to the RF field detected.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be understood and appreciated more fully from the following detailed description, taken in conjunction with the drawings in which:

FIG. 1 is a schematic illustration of one embodiment in which a seller authenticates a tag coupled to a product using an authentication device;

FIG. 2 illustrates schematically one embodiment in which a communication module is utilized to establish a communication between the product to be authenticated and the buyer;

FIG. 3 illustrates schematically one embodiment in which the communication module is utilized to establish a communication between the product to be authenticated and an authentication server;

FIG. 4 is an activation and messaging diagram of one authentication protocol according to which the buyer initiates the authentication and the authentication certificate is stored by the authentication server;

FIG. 5 is an activation and messaging diagram of one authentication protocol according to which the buyer initiates the authentication;

FIG. 6 is an activation and messaging diagram of one authentication protocol according to which a remote user initiates the authentication;

FIG. 7 is an activation and messaging diagram of one authentication protocol according to which the seller initiates the authentication and the authentication certificate is stored by the seller;

FIG. 8 is an activation and messaging diagram of one authentication protocol according to which the seller initiates the authentication and the authentication certificate is stored by the authentication server;

FIG. 9 illustrates schematically a prior art tag used for the execution of product authentication, using a cellular phone handset;

FIG. 10 illustrates schematically a tag according to the present disclosure providing overvoltage protection from excessive power input to the antenna from the mobile phone transmission; and

FIG. 11 illustrates a tag according to the present disclosure, providing a number of novel features not present in the tags of FIG S. 9 and 10.

DETAILED DESCRIPTION

Referring now to the figures, FIG. 1 is a schematic illustration of one embodiment in which a seller 105 requests an authentication of a tag 102 coupled to a product 100 using an authentication device 104, such as a mobile phone. The authentication device 104 communicates with an authentication server 106, which authenticates the tag 102 and thereby authenticates its associated product 100. A buyer 109 is able to communicate with the authentication server 106 using a communication device 108, which may also be an authentication device, such as a mobile phone or a computer. After receiving the product 100, the buyer 109 is able to verify that he received the specific ordered product 100 by communicating with the authentication server 106 using his authentication device 108.

Optionally, the authentication process is initiated by the buyer's communication device 108 initiating the authentication device 104, as shown in path 112.

In one embodiment, the authentication device 104 and/or the communication device 108 communicate with the authentication server 106 utilizing cellular communication, such as GPRS, wired communication, the Internet, or by utilizing any other appropriate communication means.

In some of the disclosed embodiments, the communication device 108 is allowed to communicate, optionally directly, with the authentication device 104 in order to initiate the authentication process of the product 100 by the authentication device 104.

In one embodiment, the communication device 108 supplies to the authentication server 106 an authentication device identification information.

Optionally, the authentication device identification information may be the phone number, network address, seller ID, or any other identification data that may enable the authentication server 106 to communicate with the authentication device 104.

Optionally, the authentication device 104 also supplies the authentication device identification information to the authentication server 106 in order for the authentication server 106 to be able to pair the communication device 108 with the authentication device 104. Then the authentication device 104 interrogates the tag 102 and sends the result to the authentication server 106, which then authenticates the tag 102 and sends the authentication result to the communication device 108.

Alternatively, the communication device 108 contacts the authentication server 106; the authentication server 106 provides the communication device 108 with a transaction identification information; the communication device 108 supplies the transaction identification information to the authentication device 104; the authentication device 104 contacts the authentication server with the transaction identification information, and that enables the authentication server to pair the authentication device 104 with the communication device 108. Then the authentication device 104 and the authentication server 106 authenticate the tag 102. And, optionally, the authentication device 104, or the authentication server 106, sends the authentication result to the communication device 108.

Optionally, the authentication server 106 accesses a server 120 holding information about the product, such as a server associated with the company that manufactures or sells the product, and provides the buyer 109 with information relevant to the product 100, such as its warranty, terms of use, support related information, etc.

Optionally, the authentication server 106 accesses a server 122 associated with a trade website, such as eBay. The trade website may rank the seller and buyer according to the transactions they make, track counterfeit products, approve only predefined products, etc.

FIG. 2 illustrates an alternative embodiment, in which a product to be authenticated 220 comprises a communication module 222, and an authentication module 224. Optionally, the communication module 222 is a cellular communication module. Alternatively, the communication module 222 is a Wireless LAN client, such as an IEEE 802.11 Wi-Fi client, or a Broadband Wireless Access client, such as an IEEE 802.16 WiMAX client.

The communication module 222 is utilized to establish a communication between the product to be authenticated 220 and the buyer 109 (through device 228). Before or after connecting with the product to be authenticated 220, the buyer 109 may connect with an authentication server 226. In order to authenticate product 220, the buyer 109 relays messages betweer the communication module 222 and the authentication server 226, optionally according to any of the above described protocols. Alternatively, the communication through the module 222 may need to be attended to by the seller 105, who, on receiving the request from the buyer 109, actuates the authentication module 224 either directly or through his authentication device 104, as in the case shown in Fig. 1.

Optionally, the authentication server 226 accesses a server 120 holding information about the product 220, such as a server associated with the company that manufactures or sells the product, and provides the buyer 109 with information relevant to the product to be authenticated 220, such as its warranty, terms of use, support related information, etc.

Optionally, the authentication server 226 accesses a server 122 associated with a trade website, such as eBay. The trade website may rank the seller and buyer according to the transactions they make, track counterfeit products, approve only predefined products, etc.

In the case where the communication module 222 is a cellular communication module, the buyer 109 may communicate directly with the product to be authenticated 220 using the cellular number. Alternatively, he may need to contact the seller 105 to actuate the authentication module 224, as in Fig. 1. In the case where the communication module 222 is a Wi-Fi or WiMAX client, the buyer 109 may obtain the network address of the communication module 222 using the unique MAC address of product 220, or using other unique information related to product 220. Optionally, the buyer 109 obtains the network address of the communication module 222 from the authentication server 226.

FIG. 3 illustrates one embodiment in which the communication module 322 is utilized to establish a communication between the product to be authenticated 320 and an authentication server 326. The authentication server 326 may authenticate the product 320 using any required protocol. Alternatively, the communication through the module 222 may need to be attended to by the seller 105, who, on receiving the request from the buyer 109, actuates the authentication module 224 either directly or through his authentication device 104, as in the case shown in Fig. 1.

Optionally, the authentication server 326 accesses a server 120 holding information about the product 320, such as a server associated with the company that manufactures or sells the product, and provides the buyer 109 (through device 328) with information relevant to the product to be authenticated 320, such as its warranty, terms of use, support related information, etc.

Optionally, the authentication server 326 accesses a server 122 associated with a trade website, such as eBay. The trade web site may rank the seller and buyer according to the transactions they make, track counterfeit products, approve only predefined products, etc.

Then the authentication server 326 may provide the results to the buyer 109 (through device 328). In the case where the communication module 322 is a cellular communication module, the communication between the product 320 and the authentication server 326 may be initiated by the buyer 109 providing the authentication server 326 with the cellular number of the communication module 322. In the case where the communication module 322 is a Wi-Fi or WiMAX client, the communication between the product 320 and the authentication server 326 may be initiated by the buyer 109 providing the authentication server 326 with the network address of the communication module 322, or with the MAC address of the communication module 322, or using other unique information related to product 320 or its communication module 322.

In one embodiment, the communication module 322 is utilized to establish a communication between the product to be authenticated 320, the buyer 109, and the authentication server 326.

A few non-limiting examples of products that may be implemented as product 320 include: (i) STB or PVR devices, which may have to communicate from time to time with a control server; (ii) devices operated by SMS or other equivalents, such as remote sensors, remote measurement devices, o: remotely operated devices; or (iii) safety or security applications, such as vehicle tracking and control mechanisms, or access control systems.

FIG. 4 is activation and messaging diagram of one authentication protocol according to which the buyer 202 initiates the authentication and the authentication certificate is stored by the authentication server 206.

The buyer 202 requests from the seller to activate 420 the authentication device in order to authenticate a product (placed close to the authentication device) with the authentication server 206 utilizing an authentication protocol 422.

Optionally, the authentication protocol 422 comprises the following steps: the buyer 202 receives the product ID from the seller 204. The buyer 202 forwards the product ID to the authentication server 206. The authentication server 206 sends the authentication challenge to the buyer 202, who forwards the challenge to the seller 204. The seller 204 sends the tag's response to the challenge to the buyer 202, who forwards the response to the authentication server 206.

Optionally, the authentication server 206 contacts 426 the brand server 208 in order to receive additional data regarding the product.

The authentication server 206 forwards 428 the authentication certificate to the buyer 202.

Optionally, the authentication server 206 updates 430 the trade website server 210, such as an eBay server, regarding the transaction.

FIG. 5 is activation and messaging diagram of one authentication protocol according to which the buyer 202 initiates the authentication.

The buyer 202 requests 520 from the authentication server 206 to activate a remote authentication protocol.

The buyer 202 receives 522 an authentication transaction identification information from the authentication server 206.

The buyer 202 forwards 524 the authentication transaction identification information to the seller 204.

The seller 204 operates an authentication protocol 526 that is based on the authentication transaction identification information it received from the buyer 202.

The authentication server 206 sends 528 the authentication result to the buyer 202.

Optionally, the authentication server 206 sends 530 the authentication result to the brand server 208.

Optionally, the authentication server 206 updates 532 the trade website server 210, such as an eBay server, regarding the transaction.

FIG. 6 is activation and messaging diagram of one authentication protocol according to which a remote user 602 initiates the authentication.

The remote user 602 requests 620 from the authentication server 206 to activate a remote authentication protocol. The remote user 602 also forwards to the authentication server 206 a verifier's identification information. The verifier 206 may also be referred to as a proxy because it is located close to the product to be authenticated. The verifier's identification information may be a phone number, a client number, a contact person's name, an e-mail address, or any other data that identifies the verifier 604.

The authentication server 206 asks 622 the verifier 604 to place his authentication device close to the product to be authenticated. In one example, the request is forwarded to the verifier 604 utilizing an e-mail, a message, an SMS, or an MMS.

Alternatively, the remote user 602 asks 624 the verifier 604 to place his authentication device close to the product to be authenticated. In one example, the remote user 602 asks the verifier 604 to do so by calling the verifier 604 or sending an e-mail, a message, an SMS, or an MMS. The system waits a predetermined duration of time until the verifier 604 authenticates the product.

The authentication server 206 authenticates 628 the product located close to the verifier 604 using the authentication protocol.

The authentication server 206 sends 630 the authentication result to the remote user 602.

Optionally, the authentication server 206 sends 632 the authentication result to the brand server 208.

Optionally, the authentication server 206 updates 634 the trade website server 210, such as an eBay server, regarding the transaction.

FIG. 7 is activation and messaging diagram of one authentication protocol according to which the seller 204 initiates the authentication and the authentication certificate is stored by the seller 204.

The seller 204 authenticates a product with the authentication server 206 utilizing an authentication protocol 720. The seller 204 receives and stores an authentication certificate 724 from the authentication server 206. Optionally, the authentication certificate comprises the following data: (i) product identification information, (ii) product description, (iii) product authentication status, such as genuine/new/used/repaired product, and (iv) certificate signature.

Optionally, the authentication server 206 utilizes data about the inquired product, which was retrieved 722 from the brand server 208, for creating the authentication certificate.

When a buyer 202 wants to buy the product, he requests 726 the authentication certificate from the seller 204.

The seller 204 forwards 728 the authentication certificate to the buyer, who contacts 730 the authentication server 206 with the authentication certificate in order to authenticate the product.

The authentication server 206 may retrieve 732 additional information related to the product from the brand server 208, such as information relevant to the buyer. And, the buyer receives 734 the relevant information from the authentication server 206.

Optionally, the authentication server 206 updates 736 the trade website server 210, such as an eBay server, regarding the transaction.

FIG. 8 is activation and messaging diagram of one authentication protocol according to which the seller 204 initiates the authentication and the authentication certificate is stored by the authentication server 206.

The seller 204 authenticates a product with the authentication server 206 utilizing an authentication protocol 820. The authentication server 206 stores the authentication certificate resulting from the authentication process, which optionally comprises the following data: (i) product identification information, (ii) product description, (iii)product authentication status, such as genuine/new/used/repaired product, and (iv) certificate signature.

The buyer 202 receives 822 the product identification information from the seller 204, and asks 824 for the authentication certificate from the authentication server 206, utilizing the received product identification information.

Optionally, the authentication server 206 contacts 826 the brand server 208 in order to receive additional data regarding the product.

The authentication server 206 forwards 828 the authentication certificate to the buyer 202. Optionally, the authentication server 206 updates 830 the trade website server 210, such as an eBay server, regarding the transaction.

Many of the embodiments are also relevant to buying products over the phone.

In one embodiment, the trade website performs the authentication process before it offers the product for sale, and receives an authentication certificate. Then the authentication certificate is signed by a public key method, such as RSA. When a potential buyer wants to verify the genuineness of the product, he sends the authentication certificate to an authentication server in order to receive a confirmation.

In one embodiment, the tag 100 is awakened by physical contact. For example, the seller may awake the tag by touching the product and/or the tag itself.

In one embodiment, the authentication process is used for supplying the user with information related and/or relevant to the interrogated product.

For example, a user may receive a coupon after authenticating a product. Alternatively, a first user may ask a second user to authenticate a product and then the first user receives a coupon or some information.

As another example, user A stands at a store and wishes to buy a cartridge for a printer he has at home. User B authenticates the printer at home and thereby the server receives the printer's properties. In order to find a cartridge matching the printer, user A places his cellular phone close to different cartridges and the phone indicates user A when it is near the right cartridge. This way the user can verify that he is buying the right product. Alternatively, the user may receive on his screen information identifying the cartridge, such as an image, name, or number. Examples for indicating the user when it is near the right cartridge include audio indications, visual indication, vibration, or a combination thereof.

Reference is now made to FIG. 9, which illustrates schematically a prior art tag 910 used for the execution of product authentication, using a cellular phone handset. The tag is intended to be attached to products whose authentication is desired. Each tag contains a unique key. The tag 910 comprises an antenna 911, which is tuned for reception of cellular phone transmission and is connected to capacitor 912 which is charged with power received by the antenna 911. The tag comprises a microprocessor 913 having a power input 914, and a short range cellular communication module 915 for transmitting data to and from a cellular phone in the vicinity, by means of Bluetooth, WiMax, WiFi or a similar system. The communication unit 915 is powered through power input 916. Both of the power inputs, 914 and 916 receive their inputs from the capacitor 912, which is charged from cellular reception antenna 911.

Reference is now made to FIG. 10, which illustrates a tag according to the present disclosure providing overvoltage protection from excessive power input to the antenna 911. The antenna 911 is optimized to absorb mobile phone energy, and by means of a charging circuit 920, charges the capacitor 912. In order to prevent the capacitor from being charged to an overvoltage, a protection switch 921, such as a gated FET, is provided between the charging circuit 920 and the capacitor 912. The gate of the FET is driven by a voltage detection circuit 924, such as a comparator receiving its input from the capacitor voltage, and with a voltage reference at its second input. When the voltage on the capacitor rises beyond the predetermined level, the FET opens, preventing the flow of further charge current onto the capacitor.

The output of the capacitor 911 provides current through a voltage regulator 926, to the tag Bluetooth microprocessor 927. Use of a voltage regulator 926, prevents the changes in voltage on the capacitor from being applied directly to the microprocessor, thus enabling the use of a smaller capacitor than would otherwise be necessary. As the microprocessor draws charge from the capacitor, the voltage on the capacitor 912 falls. When it falls below a second (lower) threshold value, this is detected by the voltage detection circuit 924, which closes the FET again, allowing the capacitor to receive charging current again.

According to a further exemplary embodiment, a sense wire 929 may be incorporated into the packaging which the tag is protecting, in a manner such that opening the package will cause the wire to tear irreversibly. The wire may be connected to the microprocessor 927 through a continuity detector 928, or a resistance monitor. By this means the microprocessor 927 can store the information that the package has been opened previously, even if it has been reclosed in a professional manner, thereby warning the purchaser of this.

According to another embodiment, it is necessary to ensure that since the mobile phone or other communication device being used to transmit and receive authentication information from a tag through its Bluetooth link, may be in the vicinity of several tags, contact is only made with the closest tag. This is advisable, since the user intends to make connection with a specific tag by holding the phone close to that tag, and a method should be provided to ensure that Bluetooth connection is only made with that tag. The Bluetooth microprocessor 927 of each tag, is equipped with a Received Signal Strength Indicator (RSSI) element, which measures the intensity of the received Bluetooth radiation from the phone. It reports the intensity value of the Bluetooth connection back to the mobile phone. Since the mobile phone can potentially make connections with a number of tags, it can thus be programmed to maintain connection only with the tag with the strongest RSSI reading.

Reference is now made to FIG. 11, which illustrates a tag according to the present disclosure, providing a number of novel features not present in previously described tags. The tag of FIG. 11 differs from that shown in FIGS. 9 and 10, where the source of energy for powering the tag is the mobile phone transmission. The tag of FIG. 11 includes an on-board battery 934. Batteries thin enough to be used on such tags and with enough energy to power such tags are available. However, their maximum current is generally very limited, typically not more than approximately 1mA. The power consumption of Bluetooth microprocessors is such that the current required during operation can get up to 30mA. However, for the small amount of data required to transfer the information, the transfer time is very short, typically only about 10 to 20 msec. Consequently, such batteries can contain sufficient energy to power the tag, but some form of buffer storage must be used so that the required current can be provided. The capacitor 912 and voltage regulator 926 of the tags previously described in this application, provide just such a current buffer. However a mechanism must be provided to ensure the proper balance between the current drain from the battery, and a sufficient current store from the capacitor.

Referring again to FIG. 11, the battery 934 is connected to the capacitor 912 through the electronically controlled switch 933, whose function will be explained hereinbelow. Switch

933 is controlled by RF activation circuitry 932, receiving its input from an antenna 931, tuned to receive mobile phone transmission. The capacitor 912 is connected via a second electronically controlled switch 936, via the Voltage Regulator 936 to the Bluetooth processor 937. Switch 936 is controlled by a voltage comparator 935. As previously, the Bluetooth processor 937 may include a Received Signal Strength Indicator (RSSI) circuit. Both of the switches may advantageously be implemented as gated FETs.

Operation of the novel features of the tag is as follows. The function of the switch 33 is to prevent waste of the energy of the battery, which is only connected to the capacitor when the switch 933 is closed. Control of the switch 933 is effected by the RF activation circuitry 920, which detects mobile phone transmissions, and generates an output signal when the detected transmission is above a predetermined level, which is an indication that a phone is being held close to the tag. This condition then closes switch 933, allowing the battery to begin charging capacitor 912. This arrangement ensures that no current is drawn from the battery unless an appropriate mobile phone transmission has been detected.

The RF activation circuitry 932 may be passive or active. If it is an active device, it can be instructed to begin operation at regular intervals of time for a certain time period set by an internal timer, which itself could be passive RC circuit. The RF activation circuitry will open the switch again after that certain period of time has elapsed.

The function of the switch 35 is to ensure that the capacitor is maintained at the correct voltage for operating the Bluetooth microprocessor. Once switch 933 has closed and the capacitor starts accumulating charge from the battery 934, it cannot commence supplying current to the microprocessor 926 until its voltage is within the working range of the microprocessor. Voltage sensor 935 detects when the voltage on the capacitor has reached a certain threshold value, and will then close switch 936 to connect the capacitor to voltage regulator 926 which will provide the correct voltage to the Bluetooth microprocessor 927 for its operation. If the voltage on the capacitor falls beneath a second threshold value, insufficient to enable the voltage regulator to provide the correct voltage to the Bluetooth microprocessor 927, switch 936 will open in order to enable the capacitor 912 to accumulate more charge and to raise its voltage to the required level.

According to another aspect of the invention, the battery will start charging the capacitor not upon automatic detection of an active mobile phone in the proximity, which is prone to error, but rather by requiring the user to touch the tag or the product package. This can be achieved either by the user pressing a switch, or by the user closing an electrical circuit through his touch. The touch sensing mechanism will thus replace the RF activation circuitry, but the rest of the circuitry will remain similar to that shown in FIG. 11. Another alternative is the use of a switch which will be closed, or a circuit activated, upon the user shaking the product. A timer mechanism can be used to cause the switch to reopen after a certain time has elapsed.

It is appreciated by persons skilled in the art that the present invention is not limited by what has been particularly shown and described hereinabove. Rather the scope of the present invention includes both combinations and subcombinations of various features described hereinabove as well as variations and modifications thereto which would occur to a person of skill in the art upon reading the above description and which are not in the prior art.

CLAIMS

1. An electronic tag comprising:

an electronic processing circuit requiring a predefined range of voltages for its operation;

a battery for supplying power for said electronic processing circuit, said battery being unable to supply the working current required by said electronic processing circuit;

a capacitor for storing charge provided by input of current from said battery;

a voltage sensing circuit for determining the voltage on said capacitor; and

an electronically controlled switch for connecting said capacitor to said electronic processing circuit,

wherein said electronically controlled switch is actuated by a signal from said voltage sensing circuit, such that said capacitor is only connected to said electronic processing circuit when the voltage developed on said capacitor is greater than a first threshold value.

2. An electronic tag according to claim 1, wherein said first threshold value is such that the voltage is sufficient to drive said electronic processing circuit.

3. An electronic tag according to either of the previous claims, further comprising a voltage regulating circuit between said capacitor and said electronic processing circuit, such that the voltage applied to power said electronic processing circuit is rendered more stable than that in a tag without said voltage regulating circuit.

4. An electronic tag according to any of the previous claims, wherein said electronically controlled switch is a field effect transistor (FET).

5. An electronic tag according to claim 4, wherein the gate of said field effect transistor is driven by the output signal from said voltage sensing circuit.

6. An electronic tag according to any of the previous claims, wherein said capacitor is disconnected from said electronic processing circuit if the voltage on said capacitor falls

below a second threshold value.

7. An electronic tag, comprising:

an electronic processing circuit requiring a predefined voltage for its operation;

a battery for supplying power for said electronic processing circuit,

a capacitor for storing charge provided by input of current from said battery;

an electronically controlled switch for connecting said battery to said capacitor; and

a mobile phone transmission detection circuit,

wherein said electronically controlled switch is actuated by a signal from said mobile phone transmission detection circuit, such that said battery is only connected to said capacitor when a mobile phone transmission of predetermined strength is detected.

8. An electronic tag according to claim 7, wherein said electronically controlled switch is a field effect transistor (FET).

9. An electronic tag according to claim 8, wherein the gate of said field effect transistor is driven by the output signal from said mobile phone transmission detection circuit.

10. An electronic tag according to any of claims 7 to 9, wherein said mobile phone transmission detection circuit is instructed to operate at regular intervals of time for a predetermined time set by said circuit.

11. A system for authenticating a product to be acquired from a first party by a second party, said system comprising:

a server comprising access to authentication data related to said product;

an authentication application operating on a first party communication device, said application being able to interrogate said server regarding the authenticity of said product;

a second party communication device capable of accessing said authentication data related to said product on said server;

wherein said system is such that an authentication request sent by said first party to said server enables said second party to authenticate said product.

12. A system according to claim 11 wherein said product is authenticated only by said second party.

13. A system according to claim 11 wherein said product is authenticated at least to said first party by means of an authentication certificate generated by said server.

14. A system according to claim 13 wherein said server generates an authentication certificate, accessible to said first party.

15. A system according to claim 13 wherein said second party retrieves said authentication certificate from said first party.

16. A system according to claim 13 wherein said second party retrieves said authentication certificate from said server.

17. A system accordi-g to any of claims 11 to 16, wherein said second party communication device and said first party communication device can communicate with each other.

18. A system according to claim 11 wherein said second party authenticates said product by having access to said authentication data on said server.

19. A system according to any of claims 11 to 18 wherein said authentication data is stored in a database on said server

20. A system according to any of claims 11 to 19 wherein at least part of said authentication data is stored in a database on a second server, to which said first server has access.

21. A system according to any of claims 11 to 20 wherein data concerning the acquiring of said product from said first party by said second party is provided to an

Internet-based trade server.

22. A system according to any of claims 11 to 21 wherein said authentication data received by said second party enables said second party to confirm that said product is genuine by communicating with either of said server or another remote server.

23. A system according to any of claims 11 to 22 wherein said server provides said second party with information about said authenticated product enabling said second party to confirm that said product provided is said authenticated product.

24. A system according to claim 23 wherein said information about said authenticated product comprises product identity information.

25. A system according to any of claims 11 to 24 wherein said product to be acquired is posted by said first party on a trade website, which is accessed by said second party.

26. A method of enabling a second party to authenticate a product offered by a first party, said method comprising;

said secona party notifying said first party of a desire to authenticate said product; and

said first party requesting authentication of said product from a server containing authentication data regarding said product; and

said server providing the result of said product authentication to said second party.

27. A method according to claim 26, wherein said result of said product authentication is provided only to said second party.

28. A method according to claim 26, wherein said result of said product authentication is provided to at least said first party in a certified manner.

29. A method according to claim 28 wherein said certified manner is performed by use of an authentication certificate.

30. A method according to claim 28, wherein said first party then provides said certified product authentication to said second party.

31. A method according to claim 28, wherein said certified product authentication resides on said server, and is accessible to said second party.

32. A method according to any of claims 26 to 31, wherein said server provides said second party with information about said authenticated product enabling said second party to confirm that said product provided is said authenticated product.

33. A method according to claim 32, wherein said information about said authenticated product enables said second party to confirm that said product is genuine by communicating with either of said server or another remote server.

34. A method according to any of claims 26 to 33, wherein said product authentication comprises:

said first party forwarding product identification information to said second party;

said second party forwarding said product identification to said server;

said server returning a challenge to said second party, who forwards said challenge to said first party ;

said first party presenting said challenge to an authentication tag associated with said product;

said first party sending said tag's response to the challenge to said second party, which forwards said response to said server for confirmation of said response.

35. A method of enabling a second party to authenticate a product offered by a first party, said method comprising;

said second party contacting an authentication server notifying it of said second party's desire to acquire said product from said first party;

said authentication server communicating with a communication module associated with said product, to activate authentication of said product;

said communication module sending said product authentication back to said server; and said server providing the result of said product authentication to said second party.

36. A method according to claim 35, wherein said first party receives from said server said second party's desire to acquire said product from said first party, and actuates authentication of said product, and said product authentication is sent back to said server for access by said second party.

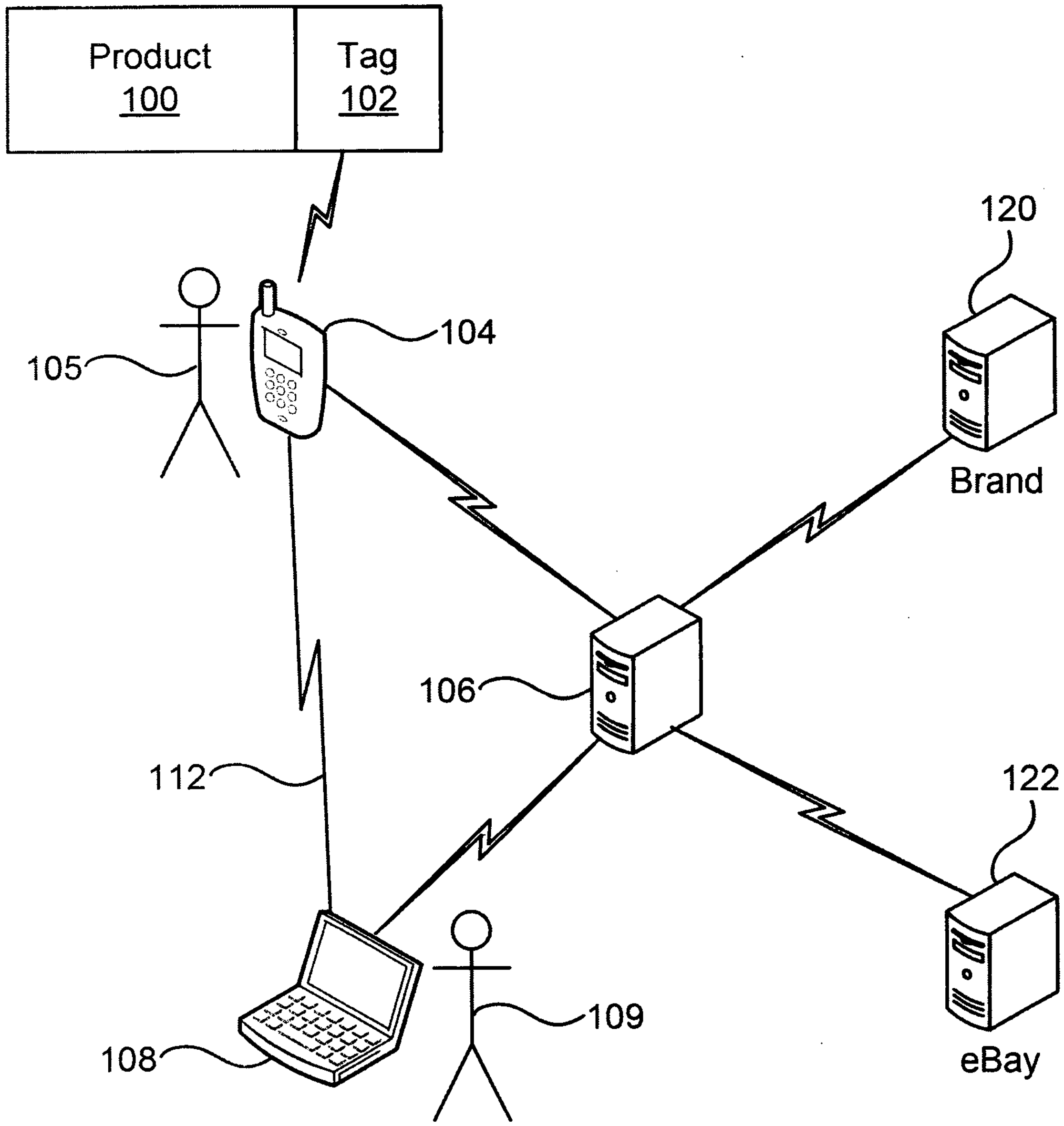

FIG. 1

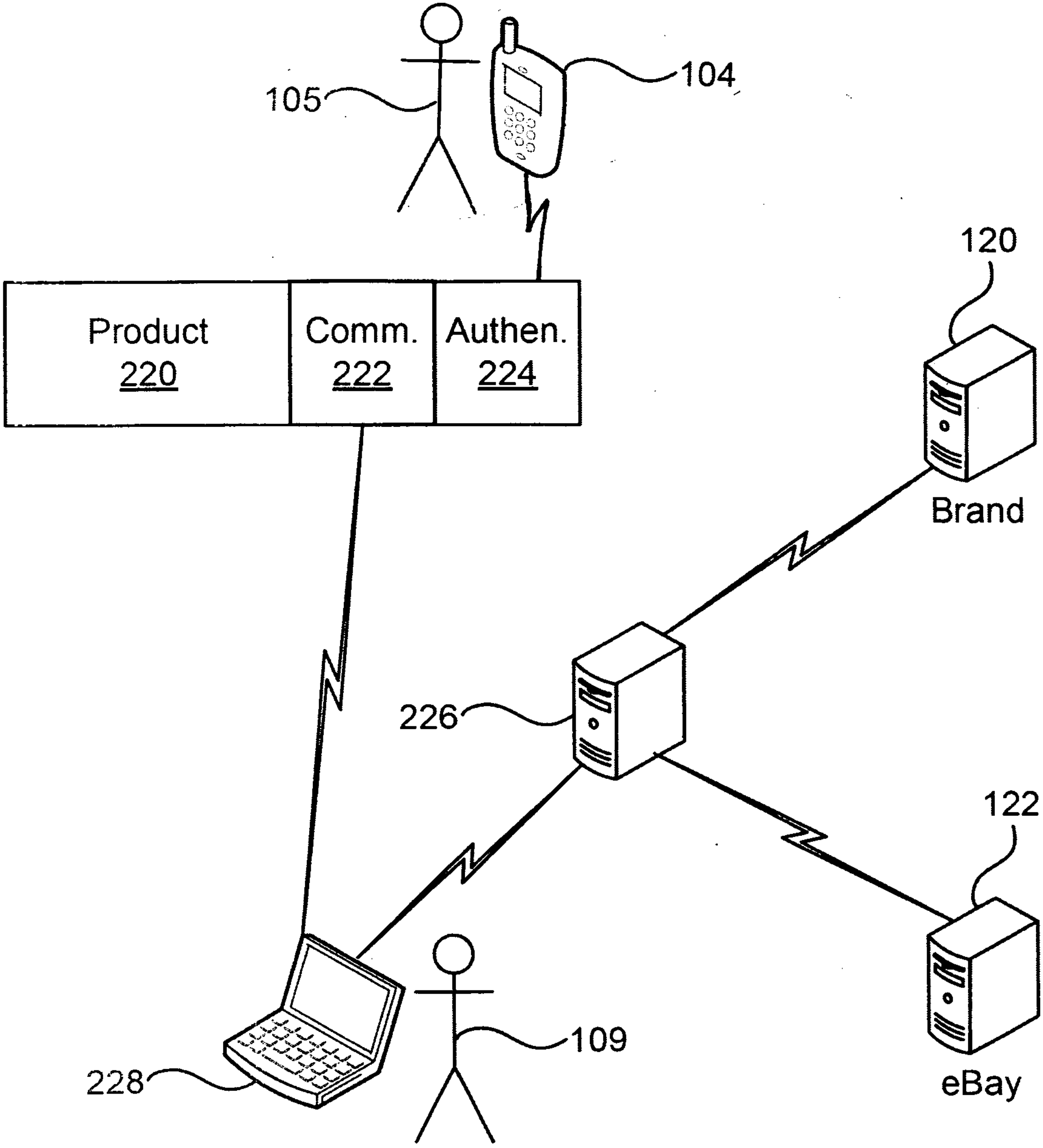
105
104
Product
220
Comm.
222
Authen.
224
120
Brand
226
122
eBay
228
109

FIG. 2

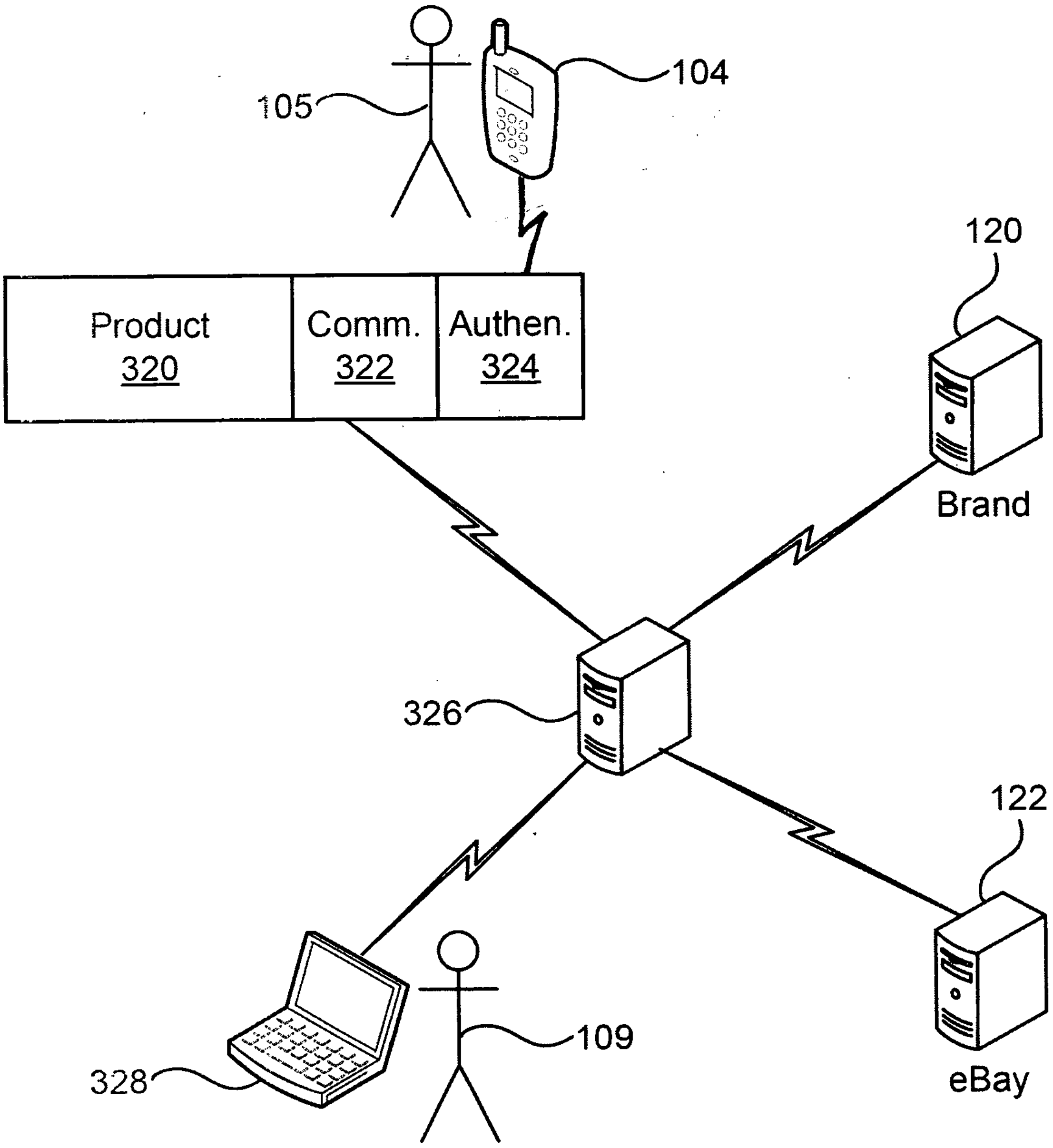
105
104
120
Product
320
Comm.
322
Authen.
324
Brand
326
122
109
328
eBay

FIG. 3

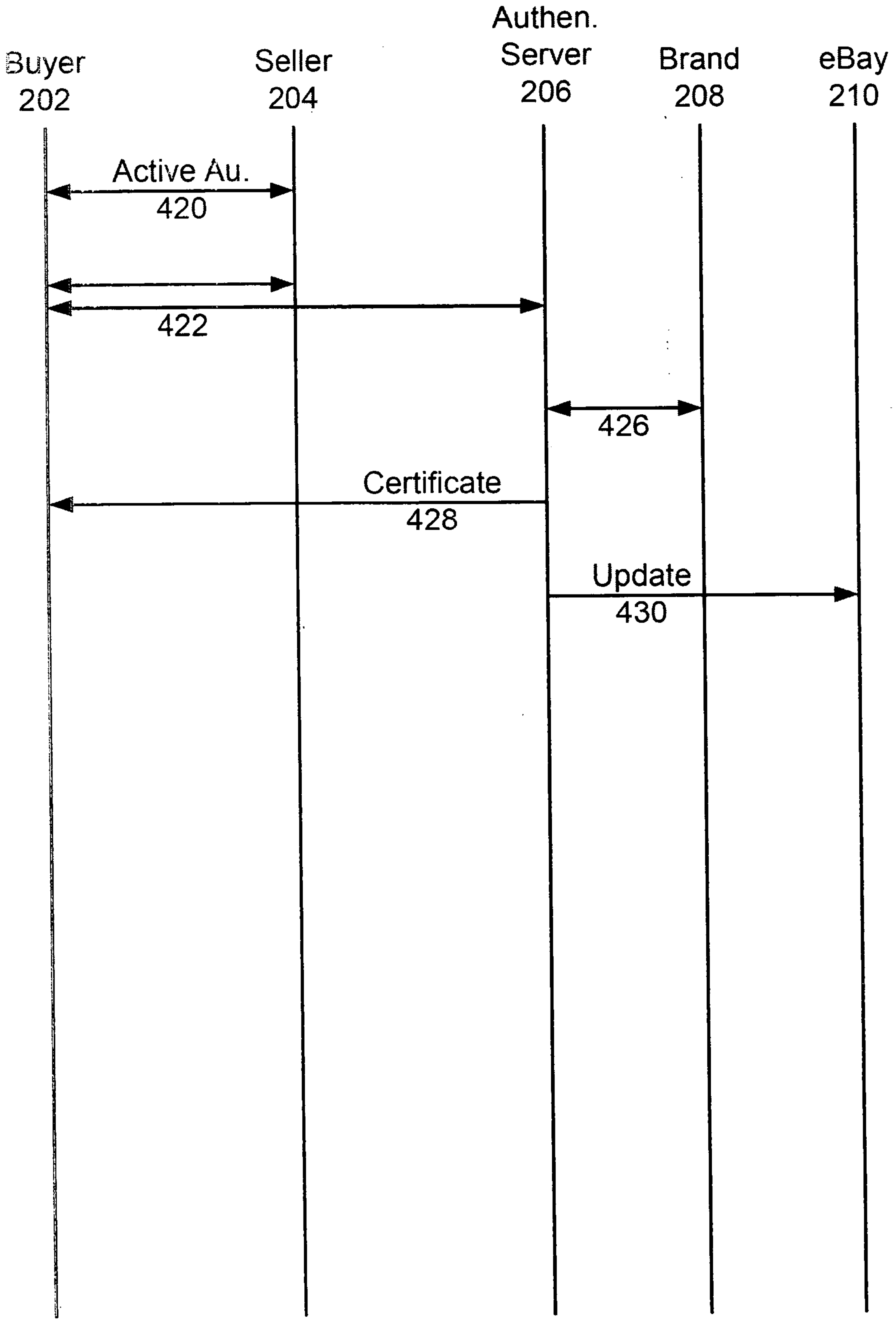
Buyer
202
Seller
204
Authen.
Server
206
Brand
208
eBay
210
Active Au.
420
422
426
Certificate
428
Update
430

FIG. 4

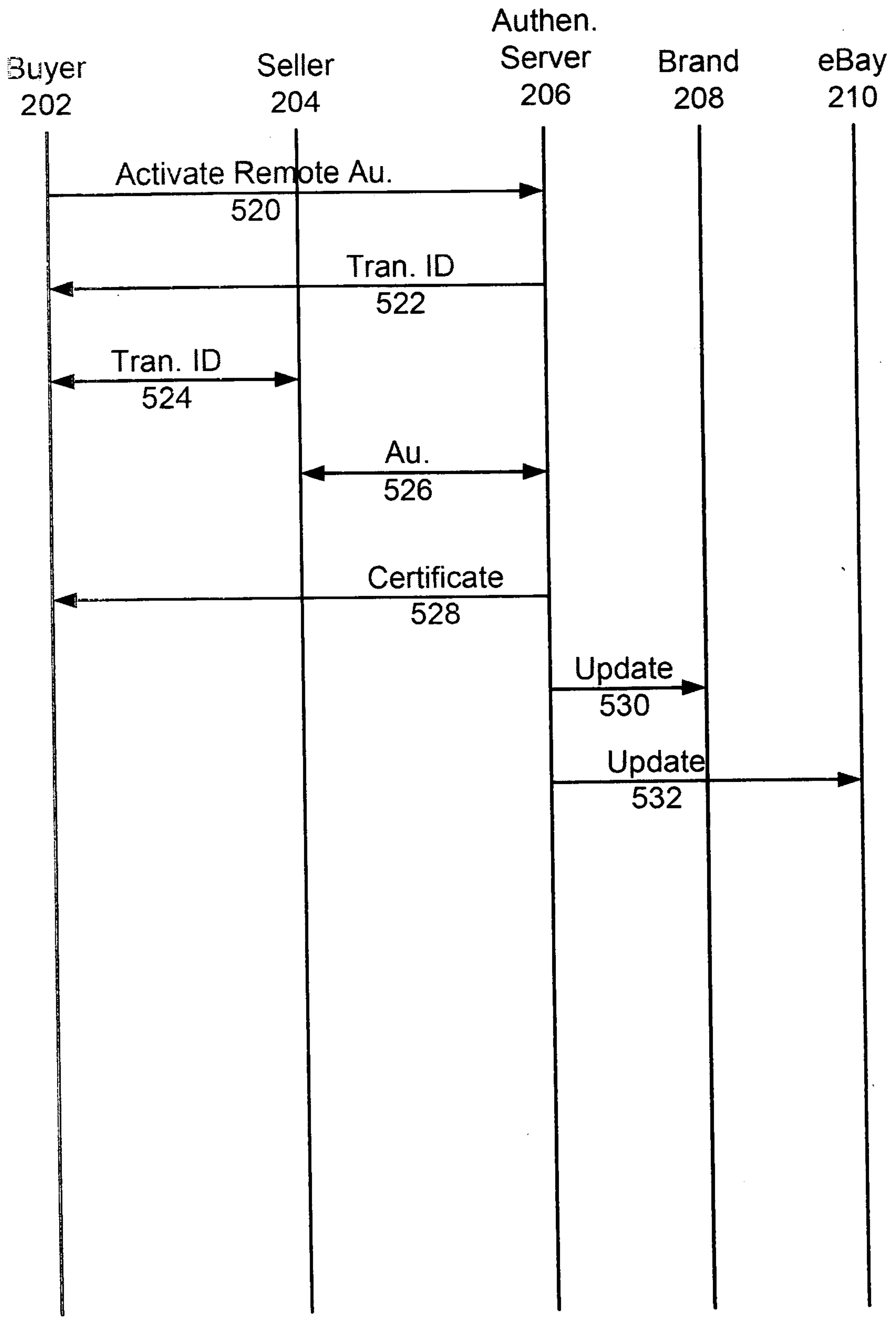
Buyer
202
Seller
204
Authen.
Server
206
Brand
208
eBay
210
Activate Remote Au.
520
Tran. ID
522
Tran. ID
524
Au.
526
Certificate
528
Update
530
Update
532

FIG. 5

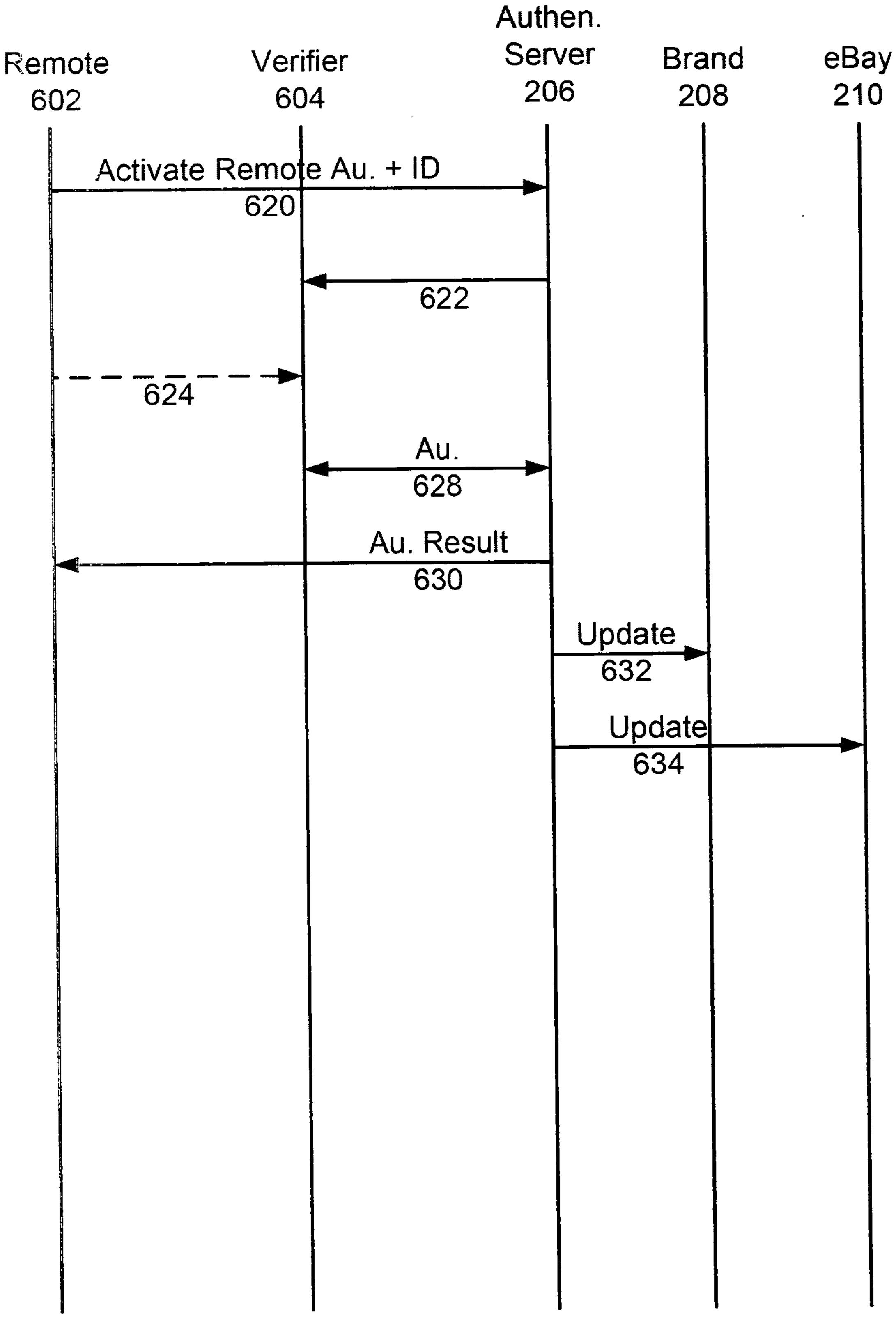
Remote
602
Verifier
604
Authen.
Server
206
Brand
208
eBay
210
Activate Remote Au. + ID
620
622
624
Au.
628
Au. Result
630
Update
632
Update
634

FIG. 6

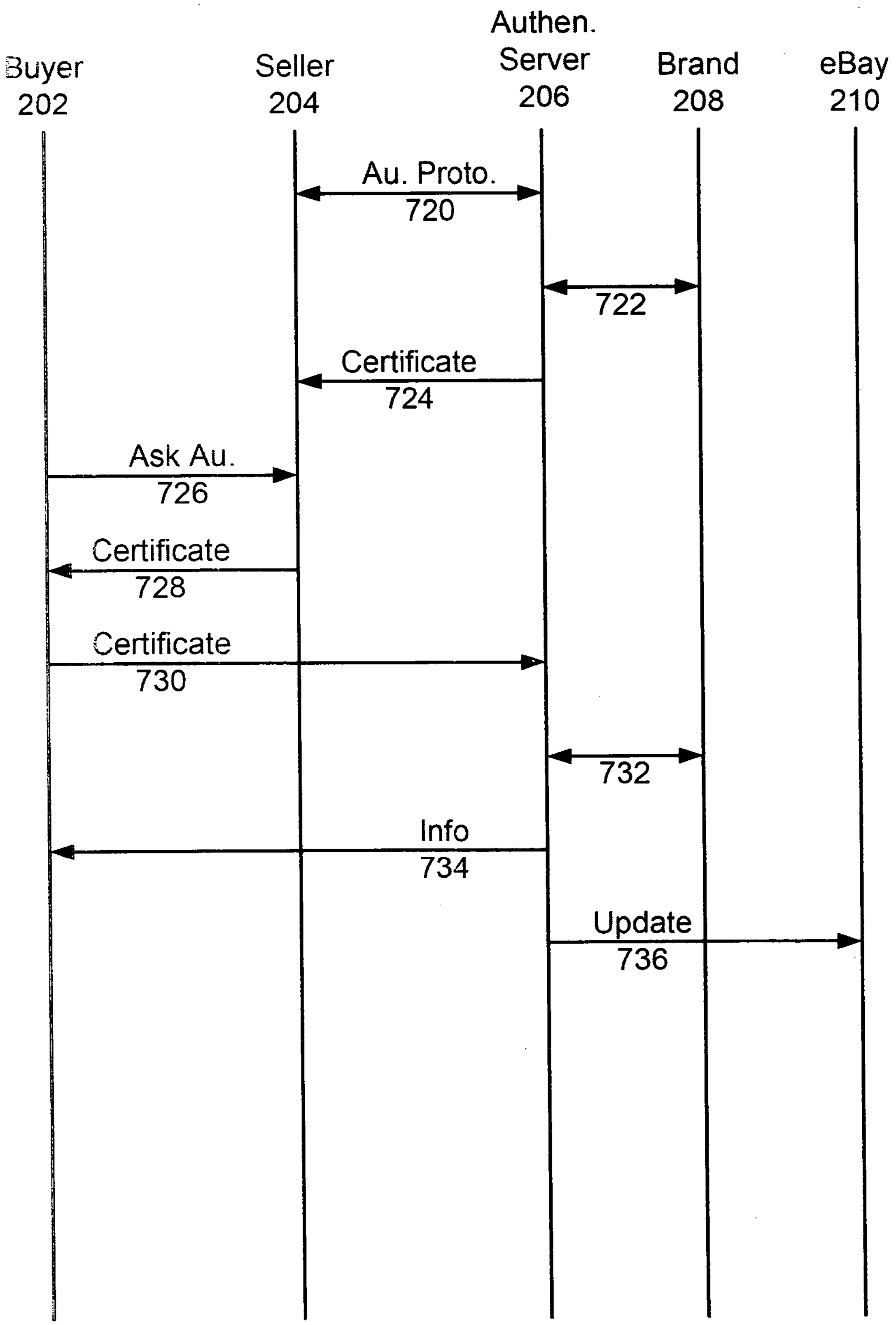
Buyer
202
Seller
204
Authen.
Server
206
Brand
208
eBay
210
Au. Proto.
720
722
Certificate
724
Ask Au.
726
Certificate
728
Certificate
730
732
Info
734
Update
736

FIG. 7

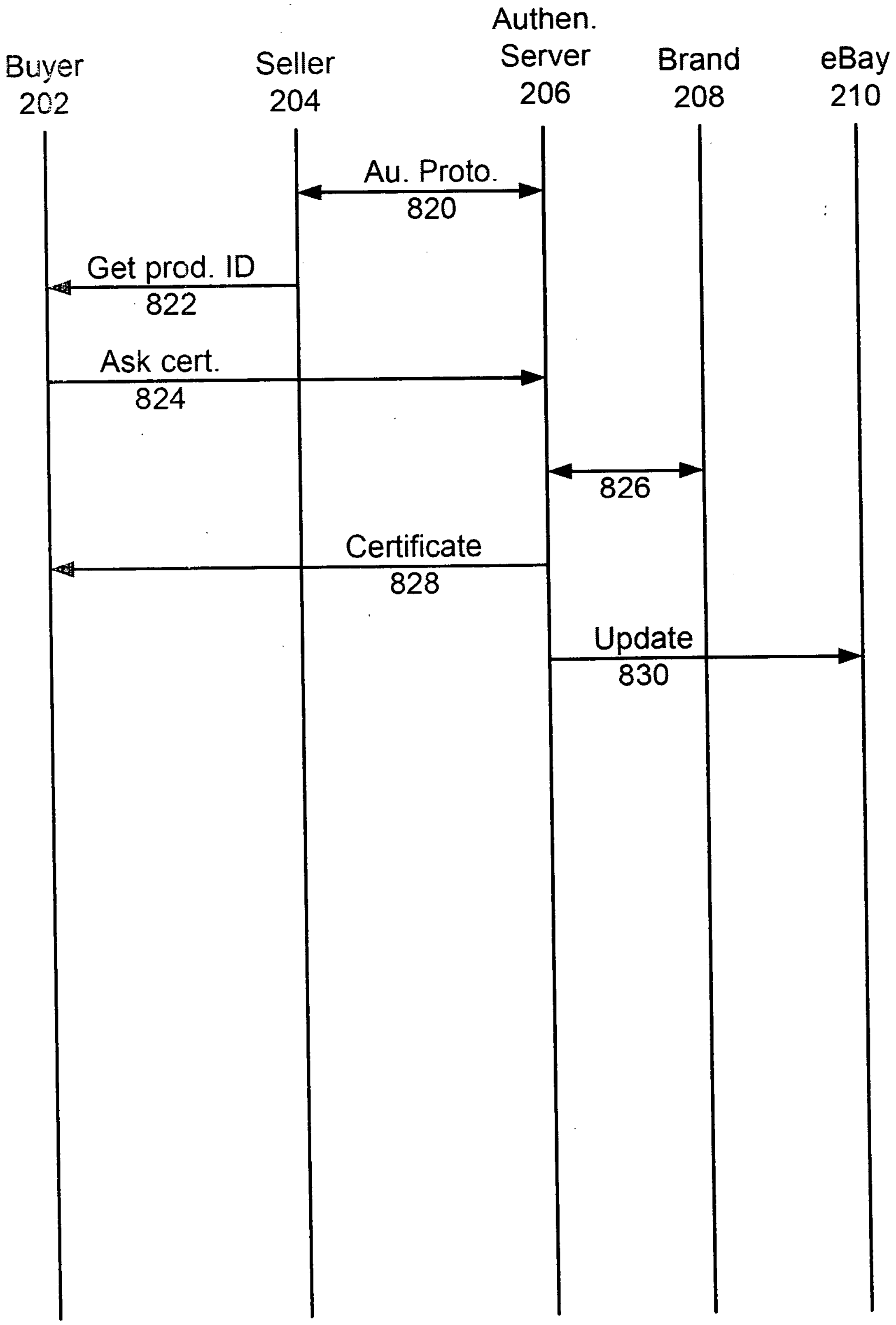
Buyer
202
Seller
204
Authen.
Server
206
Brand
208
eBay
210
Au. Proto.
820
Get prod. ID
822
Ask cert.
824
826
Certificate
828
Update
830

FIG. 8

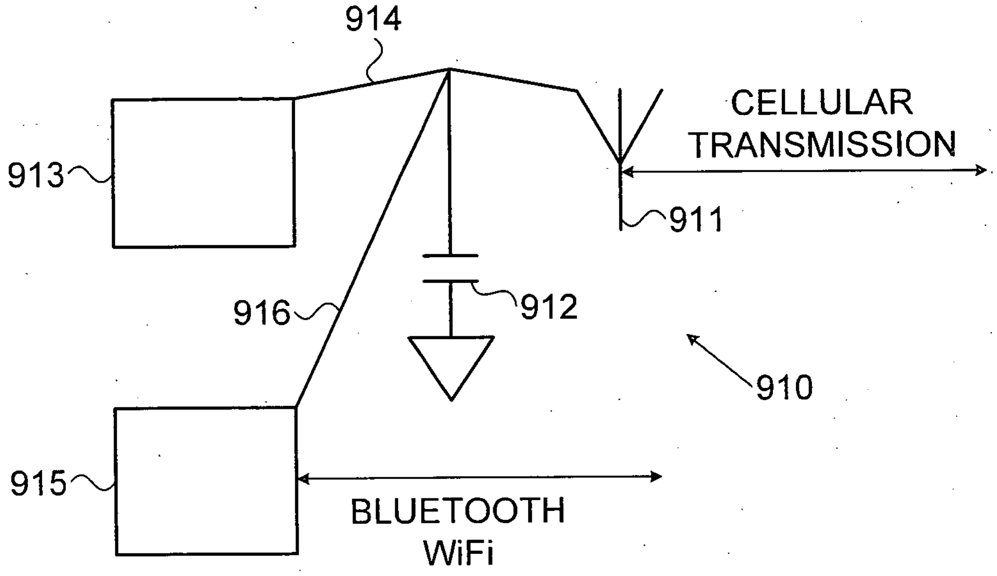

FIG. 9 (PRIOR ART)

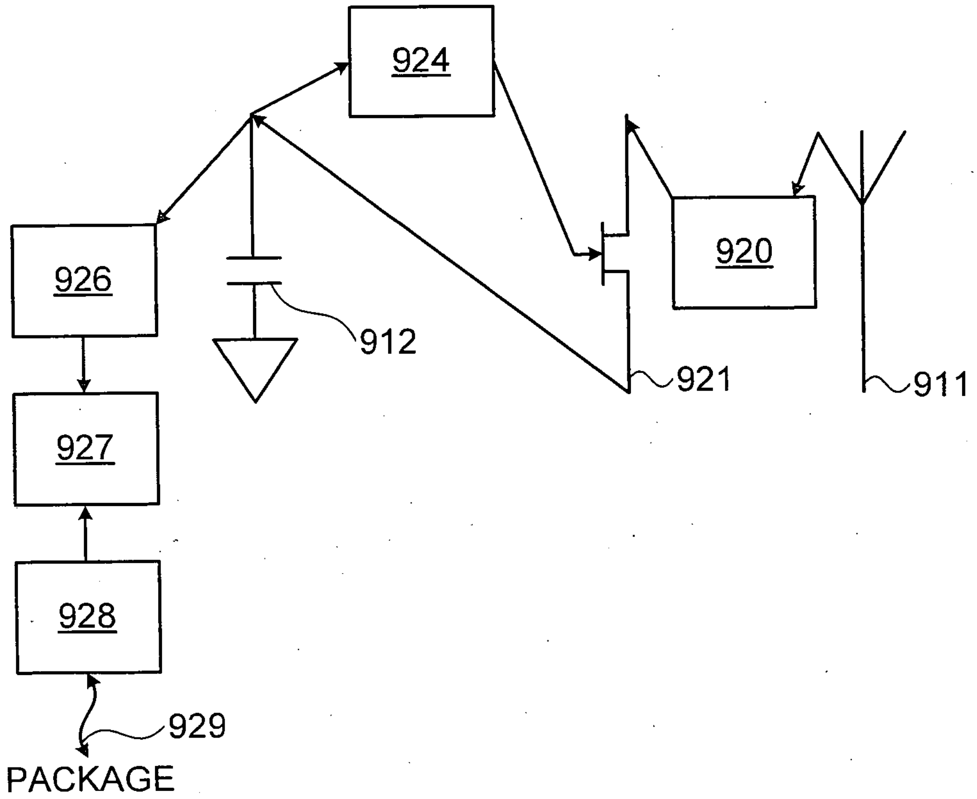

FIG. 10

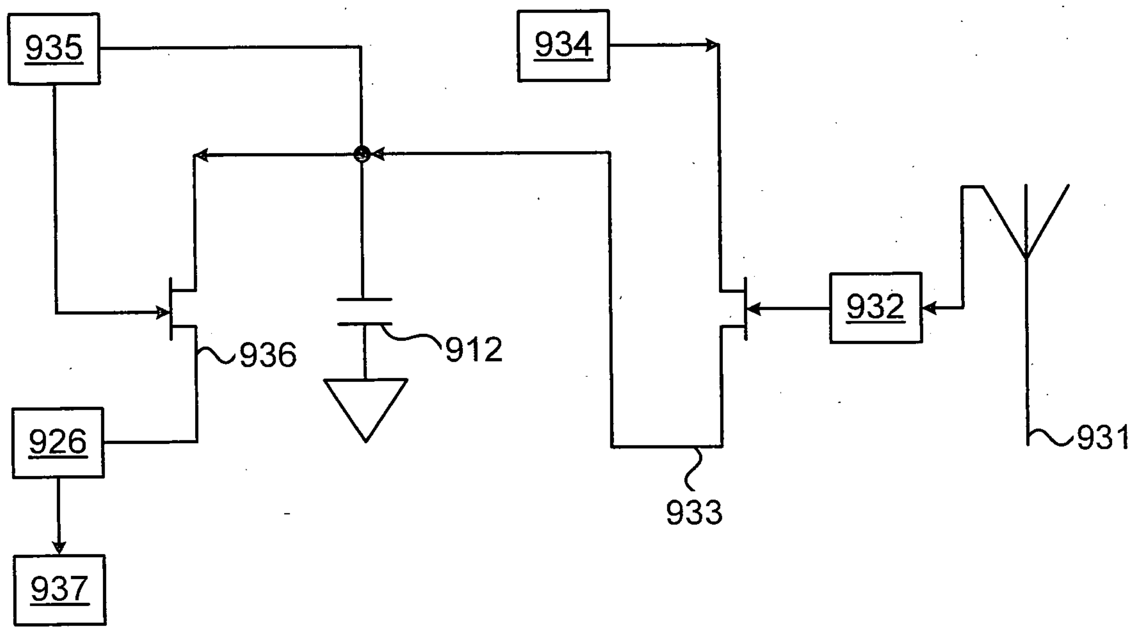

FIG. 11