Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2633882 A1 2007/06/21

(21) 2 633 882

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2006/10/16
(87) Date publication PCT/PCT Publication Date: 2007/06/21
(85) Entrée phase nationale/National Entry: 2008/06/10
(86) N° demande PCT/PCT Application No.: EP 2006/067458
(87) N° publication PCT/PCT Publication No.: 2007/068519
(30) Priorité/Priority: 2005/12/15 (EP05301063.3)

(51) Cl.Int./Int.Cl. *G06K 19/00* (2006.01),
H04L 9/32 (2006.01)

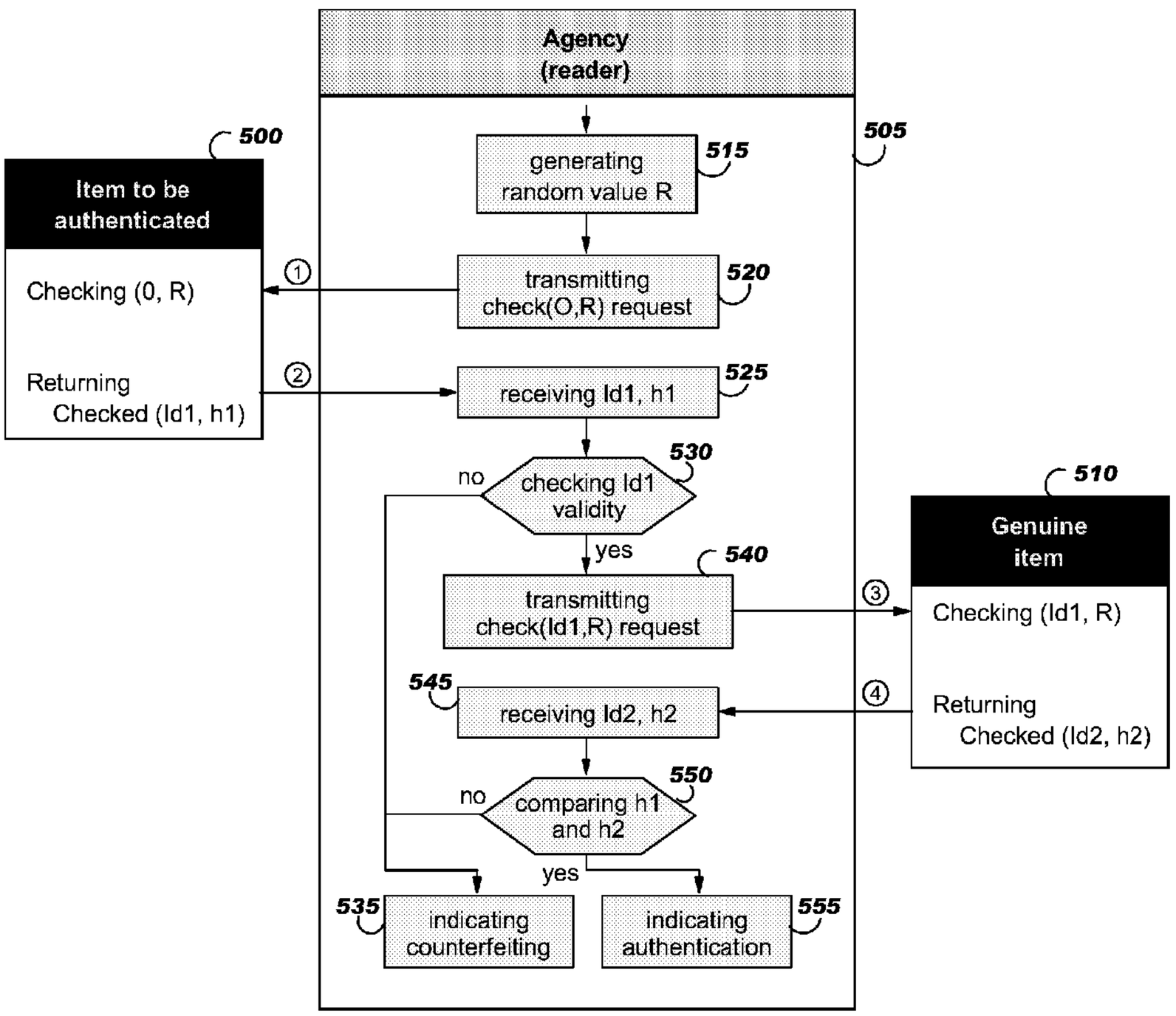
(71) Demandeur/Applicant:
INTERNATIONAL BUSINESS MACHINES CORPORATION, US

(72) Inventeurs/Inventors:
BAUCHOT, FREDERIC, FR;
CLEMENT, JEAN-YVES, FR;
MARMIGERE, GERARD, FR;
SECONDO, PIERRE, FR

(74) Agent: WANG, PETER

(54) Titre : METHODE ET SYSTEMES METTANT EN OEUVRE DES ETIQUETTES A IDENTIFICATEUR PAR RADIO FREQUENCE AFIN DE COMPARER ET D'AUTHENTIFIER DES OBJETS

(54) Title: METHOD AND SYSTEMS USING RADIO FREQUENCY IDENTIFIER TAGS FOR COMPARING AND AUTHENTICATING ITEMS



(57) Abrégé/Abstract:
A method for authenticating an item comprising an RFID having a memory for storing an identifier and a secret key, and a built-in hashing function, is disclosed. According to the method of the invention, the output of the RFID of the item to be authenticated is

CA 2633882 A1 2007/06/21

(21) 2 633 882

(13) A1

(57) Abrégé(suite)/Abstract(continued):
compared with the output of the RFID of a genuine item. To that end, a random number is transmitted to the item to be authenticated with zero as parameters. The RFID 's identifier, the random number, and the secret key are concatenated and use as input of the built-in hashing function that result is output with the RFID identifier. The RFID 's identifier and the random number are then transmitted to the RFID of the genuine item that returns its identifier and the output of the built-in hashing function computed with the RFID 's identifier of the item to be authenticated, the random number, and the secret key. If the results of both built-in hashing functions are identical, the item is authenticated else, it is counterfeiting.

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 June 2007 (21.06.2007)

PCT

(10) International Publication Number
WO 2007/068519 A3

(51) International Patent Classification:
G06K 19/00 (2006.01) *H04L 9/32* (2006.01)

(21) International Application Number:
PCT/EP2006/067458

(22) International Filing Date: 16 October 2006 (16.10.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
05301063.3 15 December 2005 (15.12.2005) EP

(71) Applicant *(for all designated States except US)*: **INTERNATIONAL BUSINESS MACHINES CORPORATION** [US/US]; New Orchard Road, Armonk, New York 10504 (US).

(71) Applicant *(for MG only)*: **COMPAGNIE IBM FRANCE** [FR/FR]; Tour Descartes, La Defense 5, 2, Avenue Gambetta, F-92400 Courbevoie (FR).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **BAUCHOT, Frederic** [FR/FR]; 299 Chemin Du Vallon, La Tourraque, F-06640 Saint-Jeannet (FR). **CLEMENT, Jean-Yves**; 1128, Chemin Du Peyrouas, F-06640 Saint-Jeannet (FR). **MARMIGERE, Gerard**; Quartier Le Patrimoine, F-06340 Drap (FR). **SECONDO, Pierre** [FR/FR]; 134, Chemin Des Berguières, F-06140 Tourrettes Sur Loup (FR).

(74) Agent: **ETORRE, Yves Nicolas**; Le Plan Du Bois, F-06610 La Gaude (FR).

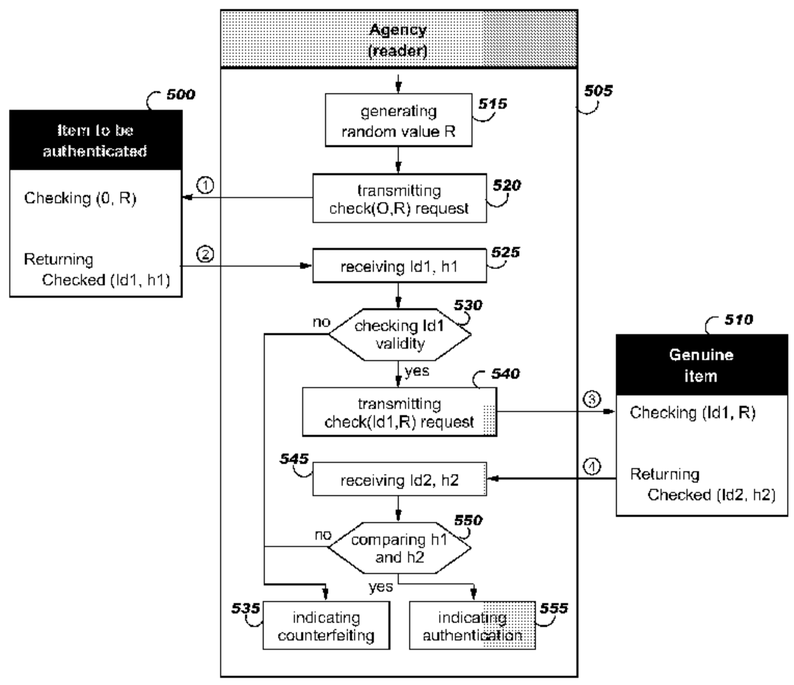
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, 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, 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, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:
— *of inventorship (Rule 4.17(iv))*

[Continued on next page]

(54) Title: METHOD AND SYSTEMS USING RADIO FREQUENCY IDENTIFIER TAGS FOR COMPARING AND AUTHENTICATING ITEMS



(57) Abstract: A method for authenticating an item comprising an RFID having a memory for storing an identifier and a secret key, and a built-in hashing function, is disclosed. According to the method of the invention, the output of the RFID of the item to be authenticated is compared with the output of the RFID of a genuine item. To that end, a random number is transmitted to the item to be authenticated with zero as parameters. The RFID 's identifier, the random number, and the secret key are concatenated and use as input of the built-in hashing function that result is output with the RFID identifier. The RFID 's identifier and the random number are then transmitted to the RFID of the genuine item that returns its identifier and the output of the built-in hashing function computed with the RFID 's identifier of the item to be authenticated, the random number, and the secret key. If the results of both built-in hashing functions are identical, the item is authenticated else, it is counterfeiting.

WO 2007/068519 A3

WO 2007/068519 A3

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
7 September 2007

METHOD AND SYSTEMS USING RADIO FREQUENCY IDENTIFIER TAGS FOR COMPARING AND AUTHENTICATING ITEMS

Field of the Invention

The present invention relates generally to method and systems for preventing counterfeiting of items and more specifically to method and systems using RFID for authenticating items by comparing the item to be authenticated with a similar genuine item.

Background of the Invention

Conventional method and apparatus exist for making it difficult to counterfeit high value items such as rare wines and perfumes, or documents such as official documents and financial document. A basic concept to assure that the item is genuine requires a form of verification of the item, such as identifiers to confirm the items as being genuine. For example, U.S. Patent Application 2004/0000987 discloses a process for detecting check fraud using Radio Frequency Identifier (RFID) tags. According to this invention, the system comprises a first device for receiving from a payor a request to create a check having a radio frequency identifier (RFID) tag associated therewith. A second device is provided for receiving from a payee a request to validate a check having an RFID tag associated therewith. The system further comprises an RFID repository. A processor is provided for (i) receiving check information from the payor, (ii) updating the RFID repository with check information received from the payor, (iii) receiving scanned check information from the payee, (iv) comparing the scanned check

information received from the payee with certain information retrieved from the RFID repository, and (v) determining if the check is valid based upon the comparison of the scanned check information received from the payee with the certain information retrieved from the RFID repository. Preferably, the RFID repository comprises a central RFID repository. Likewise, U.S. Patent 6,226,619 discloses a method and system for preventing counterfeiting of an item, including an interrogatable tag attached to the item. The item includes visible indicia for comparison with secret, non-duplicable information stored in the tag designating authenticity.

According to these methods and systems, it is possible to ensure that a given document has been issued by the relevant person, or that an item has been manufactured by the relevant manufacturer, or that a given official document has been issued by the relevant administration. As mentioned above, these methods and systems are based upon identifiers encoded within the RFIDs however, such identifiers can be duplicated on other RFIDs using a RFID scanner and writer.

Therefore, there is a need for a method and systems for improving authentication.

Summary of the Invention

Thus, it is a broad object of the invention to remedy the shortcomings of the prior art as described here above.

It is another object of the invention to provide an improved method and systems for ascertaining that an item has been produced, issued, or manufactured by the

administration, the person, or the manufacturer entitled to do so, using a radio frequency tag identifier.

It is a further object of the invention to provide an improved method and systems for ascertaining that an item has been produced, issued, or manufactured by the administration, the person, or the manufacturer entitled to do so, by comparing the item to be authenticate with a similar genuine item, using a radio frequency tag identifier.

It is still a further object of the invention to provide an improved method and systems for ascertaining that an item has been produced, issued, or manufactured by the administration, the person, or the manufacturer entitled to do so, using a radio frequency tag identifier that content is hardly duplicable.

The accomplishment of these and other related objects is achieved by a RFID for authenticating an item to which said RFID is associated, said RFID having a memory storing an identifier and a secret key, and a built-in hashing function, said RFID being adapted for,

- receiving a check command comprising two arguments *a* and *b*;

- setting the value of said parameter *a* to the value of said identifier if said parameter *a* is received equal to zero;

- concatenating said arguments *a* and *b* with said secret key in a variable C;

- computing the result H of said built-in hashing function having said variable C as input; and,

- transmitting the value of said identifier and said result H,

and by a method for authenticating a first item comprising an RFID as described above, using the reference and the RFID of a second item, said RFID of said second item being as described above and said second item being a genuine item, said method comprising the steps of,

- generating a random number;

- transmitting a first request with zero and said random number R as arguments, to said first item;

- receiving two values in response to said first request from said first item;

- transmitting a second request with the first of said two values and said random number as arguments, to the RFID of said second item;

- receiving two values in response to said second request from the RFID of said second item;

- comparing the second values of said two values received from said first item and said RFID of said second items.

Further embodiments of the invention are provided in the appended dependent claims.

Further advantages of the present invention will become apparent to the ones skilled in the art upon examination of the drawings and detailed description. It is intended that any additional advantages be incorporated herein.

Brief Description of the Drawings

Figure 1 depicts an example of the architecture of a passive RFID tag.

Figure 2 comprises figures 2a and 2b. Figure 2a shows an RFID system with a reader having an antenna and an RFID tag having a dipole antenna. Figure 2b illustrates the signal emitted by the antenna of the reader and the modulated signal reflected by the RFID tag.

Figure 3 is a flow chart diagram illustrating the logic operating in the RFIDs attached to the items to be authenticated, according to the method of the invention.

Figure 4 illustrates the main steps for preparing the items to be authenticated.

Figure 5 depicts the method of the invention for authenticating an item, based upon the comparison of the item RFID's response with the RFID's response of a genuine item.

Figure 6 is a book comprising the references and the RFIDs of genuine items, used for authenticating items without requiring the complete genuine items.

Detailed Description of the Preferred Embodiment

According to the invention, a Radio Frequency IDentifier (RFID) tag is embedded within the item to authenticate. Such RFID is preferably a short reading distance range RFID e.g., a RFID running at 13.56 MHZ. Each RFID comprises a memory for storing a unique identifier, such as an EPC, referred to as MyId in the following, a secret key, referred to as SK in the following, and a built-in function which returns a result H(x) when being fed by a variable x, where H(x) is the hashing of the input variable x according to an algorithm such as "The MD5 Message-Digest Algorithm", RFC 1321 from R.Rivest, or the "Secure Hash Algorithm 1", RFC 3174.

RFID systems

The core of any RFID system is the 'Tag' or 'Transponder', which can be attached to or embedded within objects, wherein data can be stored. An RFID reader, generically referred to as reader in the following description, sends out a radio frequency signal to the RFID tag that broadcasts back its stored data to the reader. The system works basically as two separate antennas, one on the RFID tag and the other on the reader. The read data can either be transmitted directly to another system like a host computer through standard interfaces, or it can be stored in a portable reader and later uploaded to the computer for data processing. An RFID tag system works effectively in environments with excessive dirt, dust, moisture, and/or poor visibility. It generally overcomes the limitations of other automatic identification approaches.

Several kinds of RFID, such as piezoelectric RFID and electronic RFID, are currently available. For example, passive RFID tags do not require battery for transmission since generally, they are powered by the reader using an induction mechanism (an electromagnetic field is emitted by the reader antenna and received by an antenna localized on the RFID tag). This power is used by the RFID tag to transmit a signal back to the reader, carrying the data stored in the RFID tag. Active RFID tags comprise a battery to transmit a signal to a reader. A signal is emitted at a predefined interval or transmit only when addressed by a reader.

When a passive High Frequency (HF) RFID tag is to be read, the reader sends out a power pulse e.g., a 134.2KHz power pulse, to the RFID antenna. The magnetic field generated is 'collected' by the antenna in the RFID tag that is tuned to the same frequency. This received energy is rectified and stored on a small capacitor within the RFID tag. When the power pulse has finished, the RFID tag immediately transmits back its data, using the energy stored within its capacitor as its power source. Generally, 128 bits, including error detection information, are transmitted over a period of 20ms. This data is picked up by the receiving antenna and decoded by the reader. Once all the data has been transmitted, the storage capacitor is discharged, resetting the RFID tag to make it ready for the next read cycle. The period between transmission pulses is known as the 'sync time' and lasts between 20ms and 50ms depending on the system setup. The transmission technique used between the RFID tag and the reader is Frequency Shift Keying (FSK) with transmissions generally comprised between 124.2kHz and 134.2kHz. This approach has comparatively good resistance to noise while also being very cost effective to implement.

RFID tags can be read-only, write-once, or read-write. A read-only RFID tag comprises a read-only memory that is loaded during manufacturing process. Its content can not be modified. The write-once RFID tags differ from the read-only RFID tags in that they can be programmed by the end-user, with the required data e.g., part number or serial number. The read-write RFID tags allow for full read-write capability, allowing a user to update information stored in a tag as often as possible in the limit of the memory technology. Generally, the number of write cycles is limited to about 500,000 while the number of read cycles is not limited. A detailed technical analysis of RFID tag is disclosed e.g., in RFID (McGraw-Hill Networking Professional) by Steven Shepard, edition Hardcover.

Figure 1 depicts an example of the architecture of a passive HF or Ultra High Frequency (UHF) RFID tag 100. As shown, the dipole antenna comprising two parts 105-1 and 105-2 is connected to a power generating circuit 110 that provides current from received signal to the logic and memory circuit 115, to the demodulator 120, and to the modulator 125. The input of demodulator 120 is connected to the antenna (105-1 and 105-2) for receiving the signal and for transmitting the received signal to the logic and memory circuit 115, after having demodulated the received signal. The input of modulator 125 is connected to the logic and memory circuit 115 for receiving the signal to be transmitted. The output of modulator 125 is connected to the antenna (105-1 and 105-2) for transmitting the signal after it has been modulated in modulator 125.

The architecture of a semi-passive RFID tag is similar to the one represented on figure 1, the main difference

being the presence of a power supply that allows it to function with much lower signal power levels, resulting in greater reading distances. Semi-passive tags do not have an integrated transmitter contrarily to active tags that comprise a battery and an active transmitter allowing them to generate high frequency energy and to apply it to the antenna.

As disclosed in "A basic introduction to RFID technology and its use in the supply chain", White Paper, Laran RFID, when the propagating wave from the reader collides with tag antenna in the form of a dipole, part of the energy is absorbed to power the tag and a small part is reflected back to the reader in a technique known as back-scatter. Theory dictates that for the optimal energy transfer, the length of the dipole must be equal to half the wave length, or $\lambda/2$. Generally, the dipole is made up of two $\lambda/4$ lengths. Communication from tag to reader is achieved by altering the antenna input impedance in time with the data stream to be transmitted. This results in the power reflected back to the reader being changed in time with the data i.e., it is modulated.

Figure 2, comprising figures 2a and 2b, shows an RFID system 200. As depicted on figure 2a, RFID system 200 comprises a reader 205 having an antenna 210. The antenna 210 emits a signal 215 that is received by an RFID tag 220. Signal 215 is reflected in RFID tag 220 and re-emitted as illustrated with dotted lines referred to as 225. Figure 2b illustrates the signal 215 emitted by the antenna 210 of the reader 205 and the signal 225 reflected by the RFID tag 220. As shown on figure 2b, the reflected signal 225 is modulated.

Behavior of the RFID embedded within an item

As mentioned above, each RFID used for authenticating an item comprises an integrated circuit implementing a memory for storing a unique identifier referred to as MyId, a secret key referred to as SK, and a built-in function H returning H(x) when being fed with variable x, H(x) being the hashing of the input variable x according to algorithms such as "The MD5 Message-Digest Algorithm" RFC 1321 from R.Rivest or "Secure Hash Algorithm 1" RFC 3174.

Each RFID, upon reception of a request for operation within its operating frequency range, operates according to the logic shown on the flow chart diagram of figure 3. When activated, the RFID is initialised and it gets its identifier MyId and the stored secret key SK from its memory (step 300). Then, the RFID waits until the reception of a check request having *a* and *b* as parameters (step 305). If parameter *a* is equal to zero (step 310), parameter *a* is set to MyId (step 315) i.e., the value of the RFID's identifier. The value of parameters *a* and *b* are then concatenated with the secret key SK in variable *C* (step 320). When concatenated, the result *C* is used as the input of the built-in hashing function that output is referred to as *h* (step 325). The RFID's identifier MyId and the result *h* of the built-in hashing function are then returned by the RFID in a checked command (step 330).

Method for tagging the items to be authenticated

When an item should be authenticated according to the method of the invention, it should comprise an RFID as the one described by reference to figure 3. A genuine item must be given to the agency or organism that will authenticate the items for comparison purpose.

Figure 4 illustrates the main steps for preparing the items to be authenticated. It involves four parties: an RFID's manufacturer (400), the organisation distributing the items to be authenticated (405), the item's manufacturer (410), and the agency or organism that will authenticate the items (415). Depending upon the items, the item's manufacturer can be the organisation distributing the items to be authenticated and/or the RFID's manufacturer can be the item's manufacturer and/or the organisation distributing the items to be authenticated. Before selling or giving the items to be authenticated, the organisation 405 distributing the items transmits a request for RFIDs, as the ones described by reference to figure 3, to the RFID's manufacturer 400, as shown with arrow having the reference ①. If a secret key does not already exists for this organisation 405, a secret key is generated. Such secret key can be generated by a specialised company. The RFIDs are then manufactured by the RFID's manufacturer according to the specifications mentioned above, using the secret key associated to the organisation 405. The RFID's identifiers are determined according to standard methods e.g., continuous numbering. The RFIDs are then shipped to the item's manufacturer 410 which integrates them into the items, as shown with arrow having the reference ②. The items comprising the RFIDs are then transmitted to the organisation 405, as shown

with arrow having the reference ③. The organisation 405 gives one genuine item to the agency or organism 415 that will authenticate the items by comparing the items with the received genuine item, as shown with arrow having the reference ④.

Method for authenticating an item

The method of the invention for authenticating an item is based upon the comparison of the item RFID's response with the RFID's response of a genuine item, as illustrated on figure 5. For authenticating an item 500, the agency 505 uses an RFID reader connected to a computer, a portable computer, a hand-held device, or the like, running the algorithm of the authenticating method. The item 500 is compared to the genuine item 510. After having generated a random number *R* according to a standard algorithm (step 515), the reader transmits a check request to the item to be authenticated (step 520), with arguments zero and *R*, as illustrated with arrow having the reference ①. As mentioned above by reference to figure 3, the RFID of the item to be authenticated concatenates the RFID's identifier, referred to as Id1, the random number *R*, and the secret key stored within the RFID, and computes the result h1 of the built-in hashing function having this concatenated value as input. Result h1 and the RFID's identifier are returned by the RFID in the checked command, as illustrated with arrow having the reference ②. After receiving the checked command with values Id1 and h1 (step 525), the reader performs a first authentication using the returned RFID's identifier Id1 (step 530). Such authentication can be done, for example, by comparing the RFID's identifier Id1 with the organisation RFID's identifiers that can be stored in a database. If the

item is not authenticated, an alert is transmitted to the user (step 535) and the authentication process is stopped. In the given example, the user is informed of counterfeiting. Such alert can be done, for example, through a display or speaker. On a display, the alert can be done with textual display such as "counterfeiting item", and/or using a predetermined colour such as a red led. Using a speaker, the alert can be done with voice synthesis such as pronouncing "counterfeiting item", and/or using a predetermined sound. If the item is authenticated, the reader transmits a check request to the genuine item (step 540), with arguments Id1 and *R*, as illustrated with arrow having the reference ③. As mentioned above by reference to figure 3, the RFID of the genuine item concatenates the item RFID's identifier Id1, the random number *R*, and the secret key stored within the RFID, and computes the result h2 of the built-in hashing function having this concatenated value as input. Result h2 and the RFID's identifier Id2 are returned by the RFID in the checked command, as illustrated with arrow having the reference ④. After receiving the checked command with values Id2 and h2 (step 545), the reader compares the values h1 and h2 (step 550). If h1 is equal to h2, the item is authenticated else, if h1 is different than h2, the item is counterfeiting. This authentication status is indicated to the user (step 535 or 555). If the item is not authenticated, the user is forewarned as described above (step 535). If the item is authenticated, an alert is transmitted to the user (step 555). Again, such alert can be done, for example, through a display or a speaker. On a display, the alert can be done with textual display such as "Authenticated item", and/or using a predetermined colour such as a green led. Using a speaker, the alert can be done with voice synthesis such as pronouncing "authenticated

item", and/or using a predetermined sound, different than the predetermined sound characterising a counterfeiting item.

As it will be obvious for the one skilled in the art in view of the present invention, the complete genuine item is not required for the comparison, only its RFID can be used. For sake of simplicity, the agency can create a kind of book comprising all the RFIDs of the genuine items to be authenticated as shown on figure 6. The book 600 comprises a plurality of pages and, on each page, one or several areas 605. Each area 605 comprises at least the genuine item's reference 610 and the genuine item's RFID 615, characterising a particular genuine item.

The main advantage and characteristic of the disclosed invention relates to the fact that the authentication is done by using a randomly generated number for proofing that the suspicious object includes an RFID tag hosting the secret key SK. Any malicious people would have to visit the whole set of randomly generated numbers to be able to build an RFID answering the expected result for any value of the input. With a random number range that is large enough, this would ask for a memory size which is not compatible with what an RFID tag can host.

Naturally, in order to satisfy local and specific requirements, a person skilled in the art may apply to the solution described above many modifications and alterations all of which, however, are included within the scope of protection of the invention as defined by the following claims.

Claims:

1. An RFID for authenticating an item to which said RFID is associated, said RFID having a memory storing an identifier and a secret key, and a built-in hashing function, said RFID being adapted for,

- receiving a check command comprising two parameters *a* and *b*;
- setting the value of said parameter *a* to the value of said identifier if said parameter *a* is received equal to zero;
- concatenating said parameters *a* and *b* with said secret key in a variable C;
- computing the result H of said built-in hashing function having said variable C as input; and,
- transmitting the value of said identifier and said result H.

2. The RFID of claim 1 wherein said RFID is a passive short reading distance range RFID.

3. A method for authenticating a first item comprising an RFID as described in claim 1 or in claim 2, using the reference and the RFID of a second item, said RFID of said second item being as described in claim 1 or in claim 2 and said second item being a genuine item, said method comprising the steps of,

- generating a random number;

- transmitting a first request with zero and said random number R as parameters, to said first item;

- receiving two values in response to said first request from said first item;

- transmitting a second request with the first of said two values and said random number as parameters, to the RFID of said second item;

- receiving two values in response to said second request from the RFID of said second item;

- comparing the second values of said two values received from said first item and said RFID of said second items.

4. The method of claim 3 wherein said first item is authenticated if said second values of said two values received from said first item and from the RFID of said second items are identical.

5. The method of either claim 3 or claim 4 further comprising the step of checking the validity of the first of said two values received from said first item.

6. The method of any one of claims 3 to 5 further comprising the step of indicating the authentication status.

7. The method of claim 6 wherein said step of indicating the authentication status comprises the step of displaying said authentication status.

8. The method of claim 6 wherein said step of indicating the authentication status comprises the step of emitting a noise characterizing said authentication status.

9. An apparatus comprising means adapted for carrying out each step of the method according to any one of the claims 3 to 8.

10. A computer-like readable medium comprising instructions for carrying out each step of the method according to any one of the claims 3 to 8.

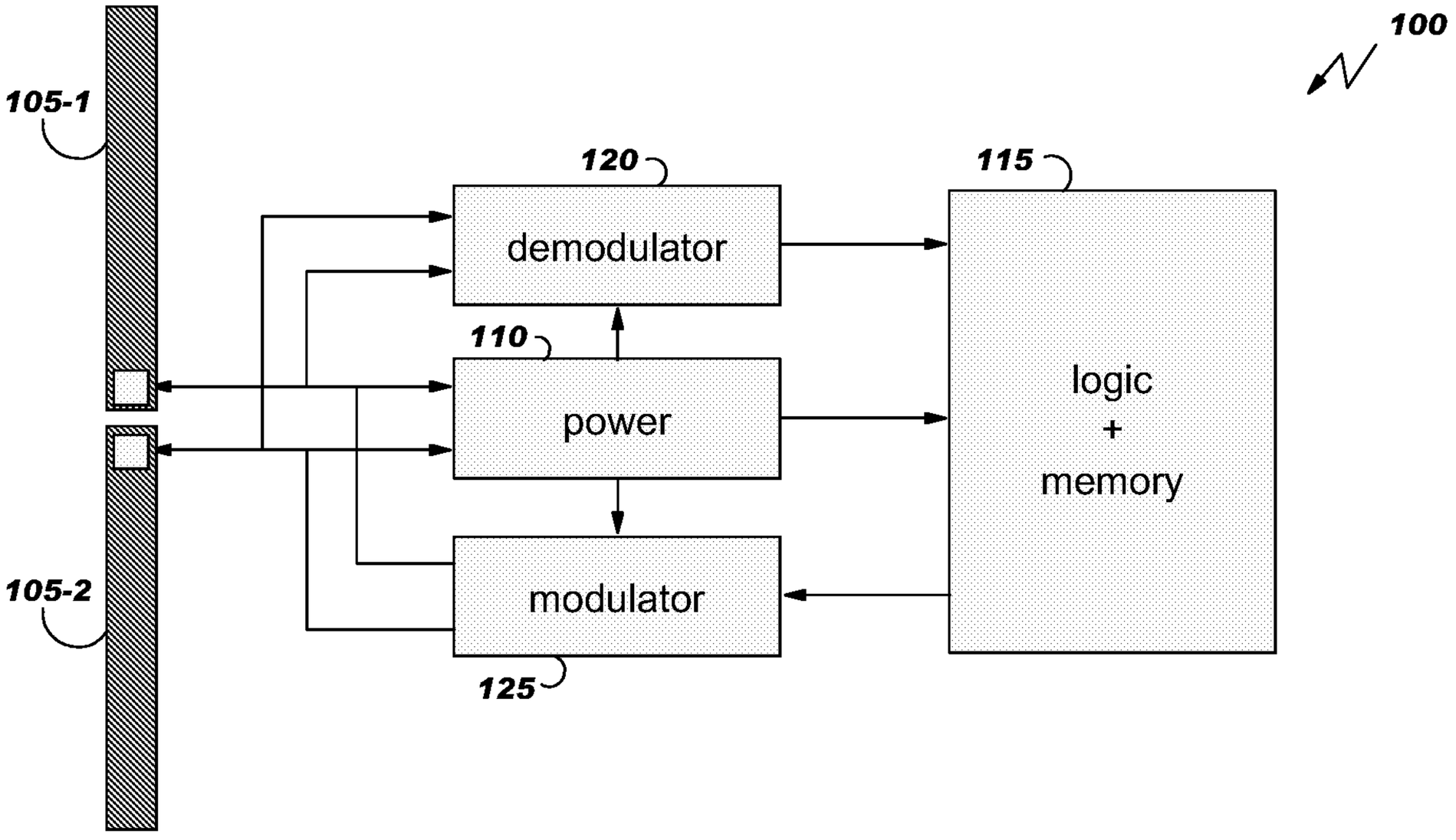


Figure 1

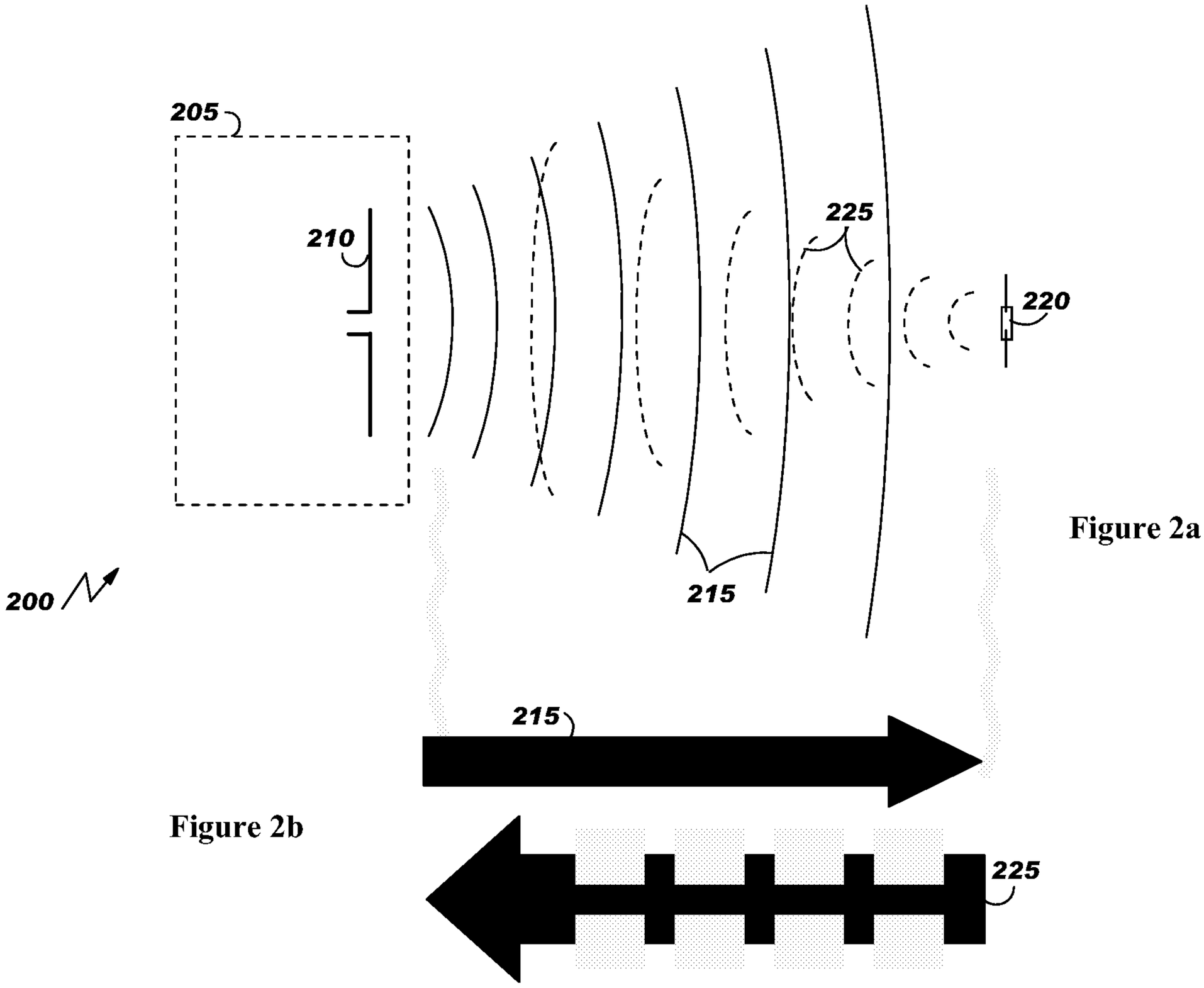


Figure 2a

Figure 2b

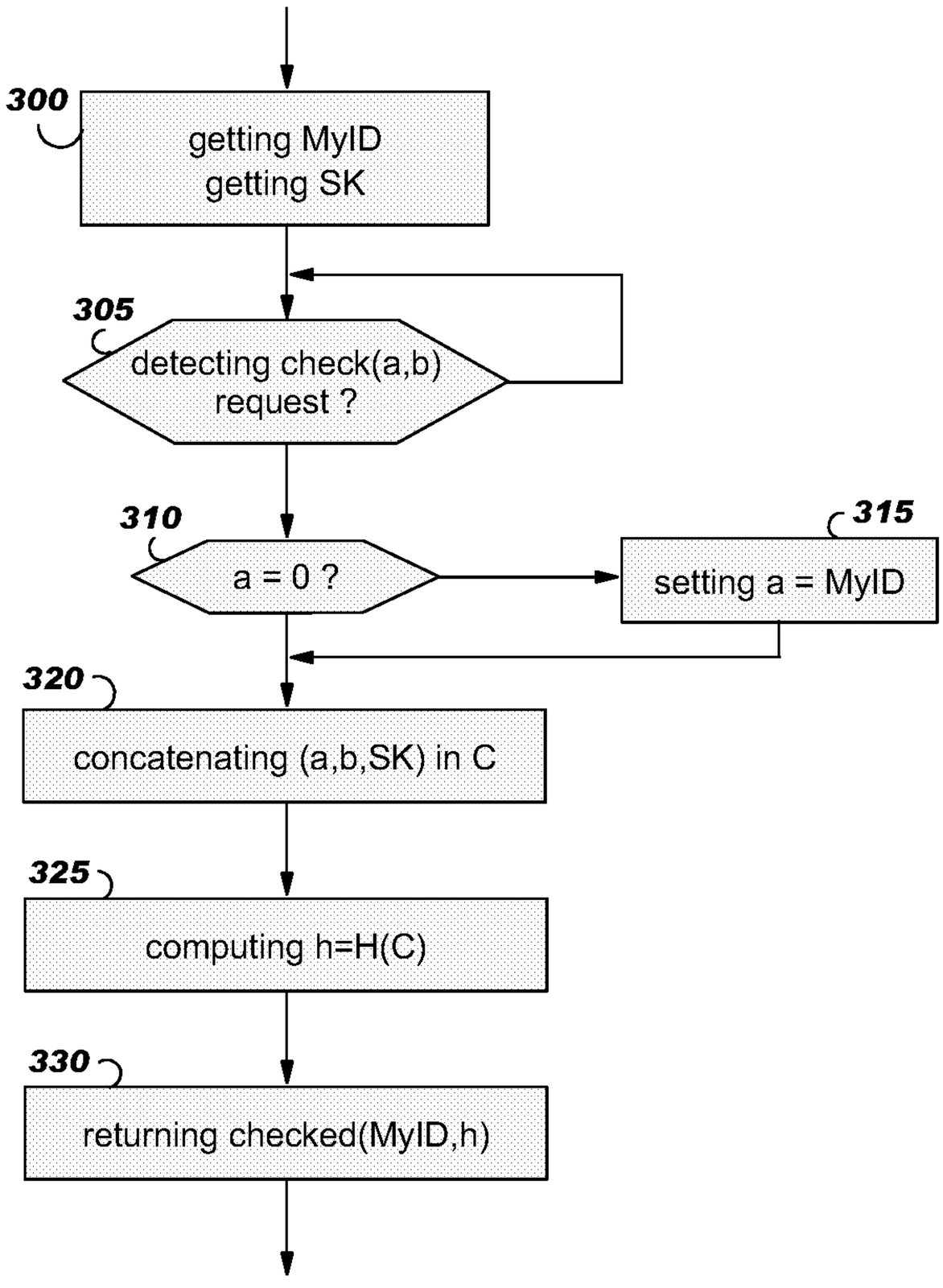


Figure 3

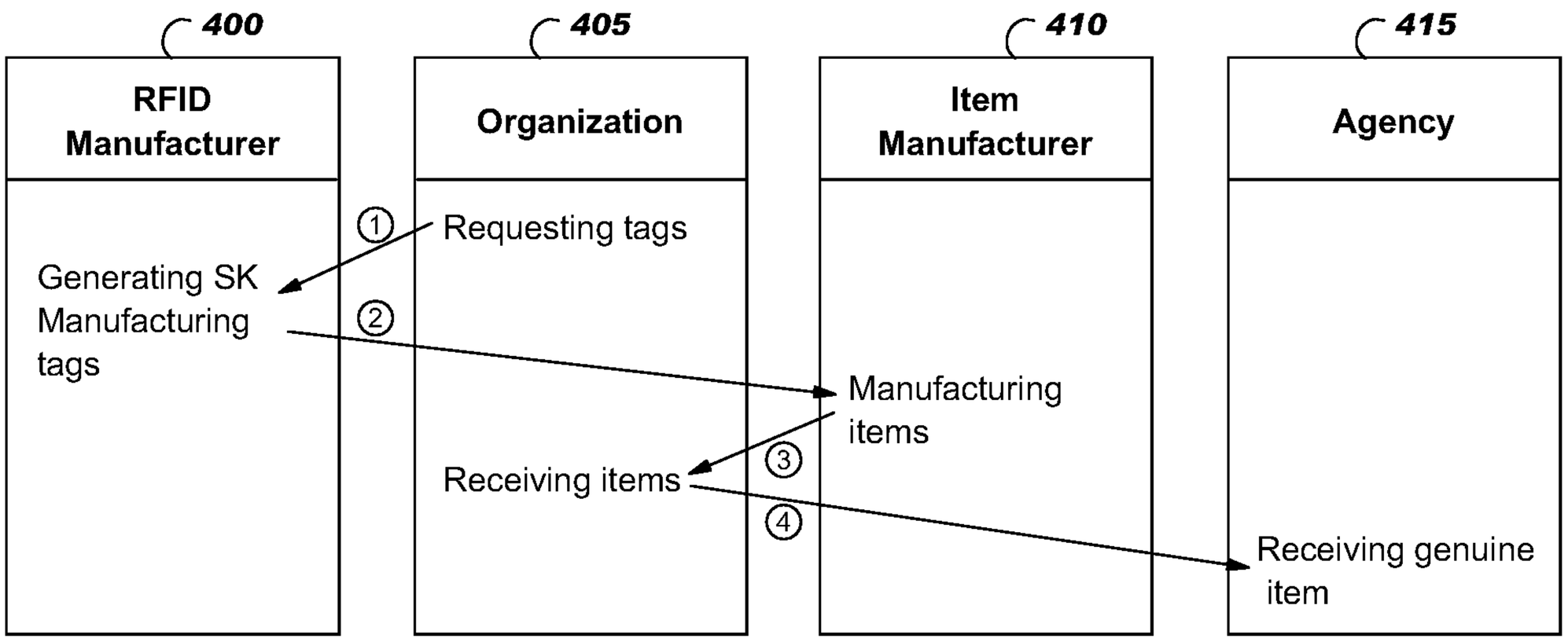


Figure 4

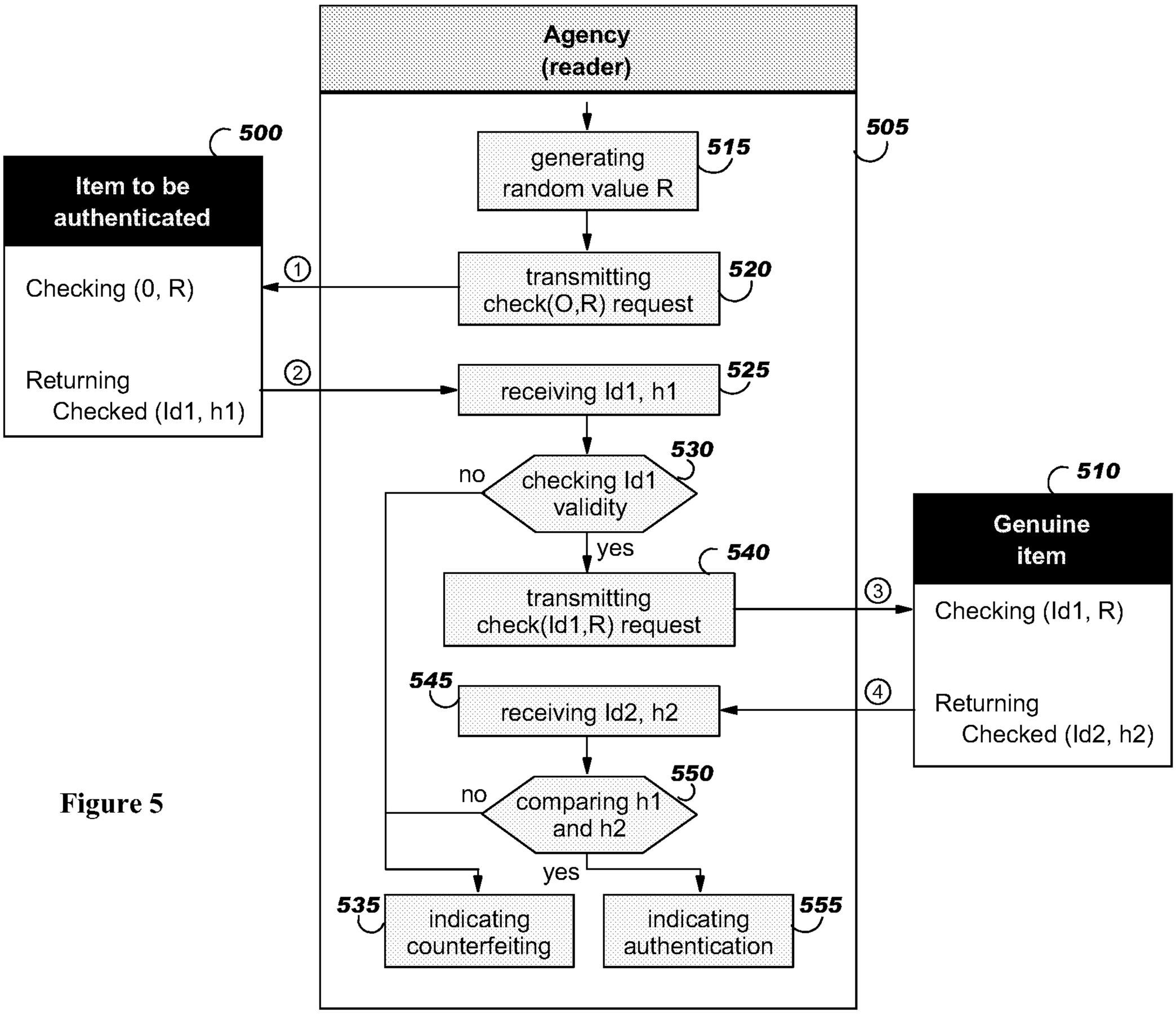


Figure 5

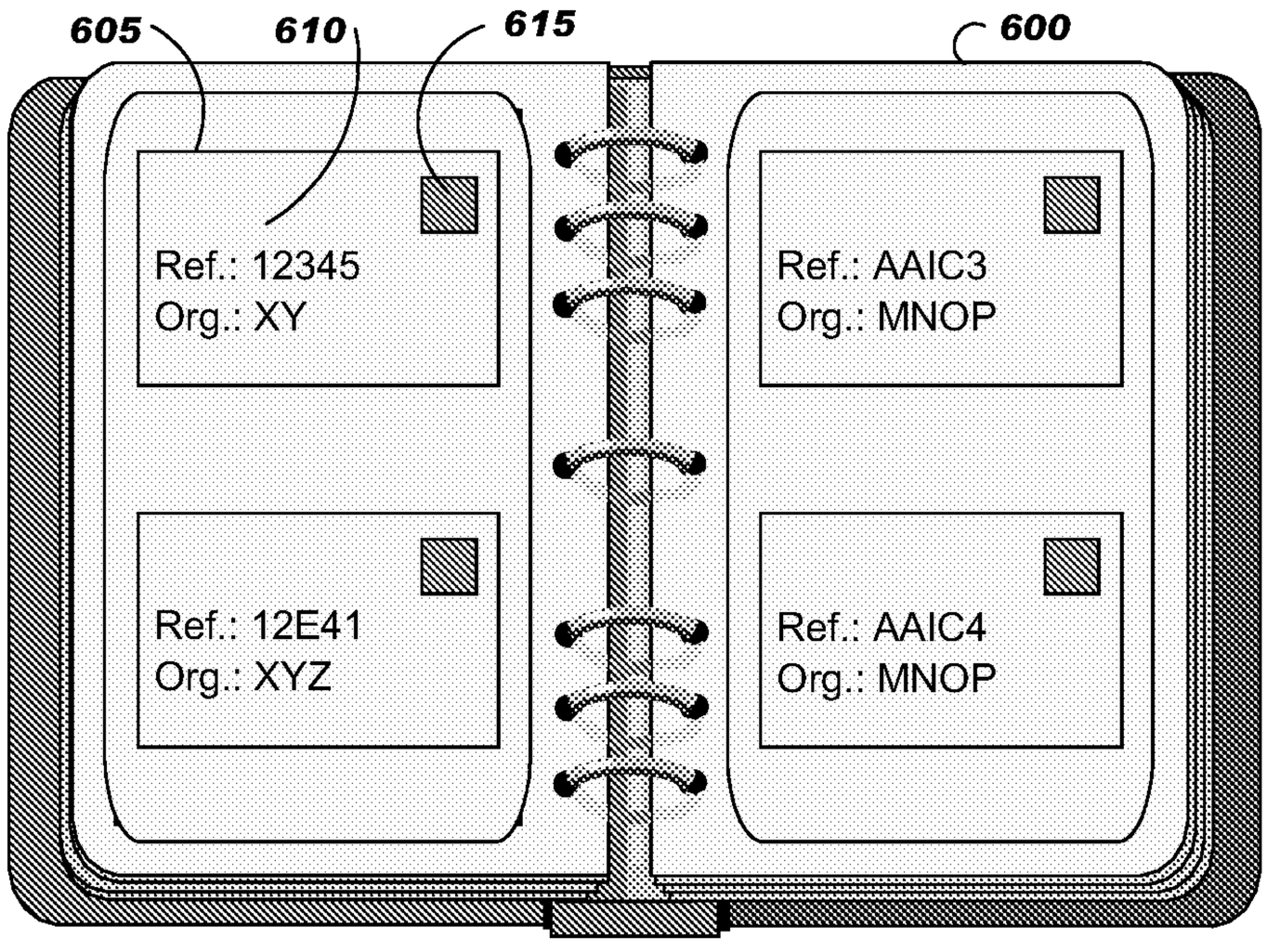
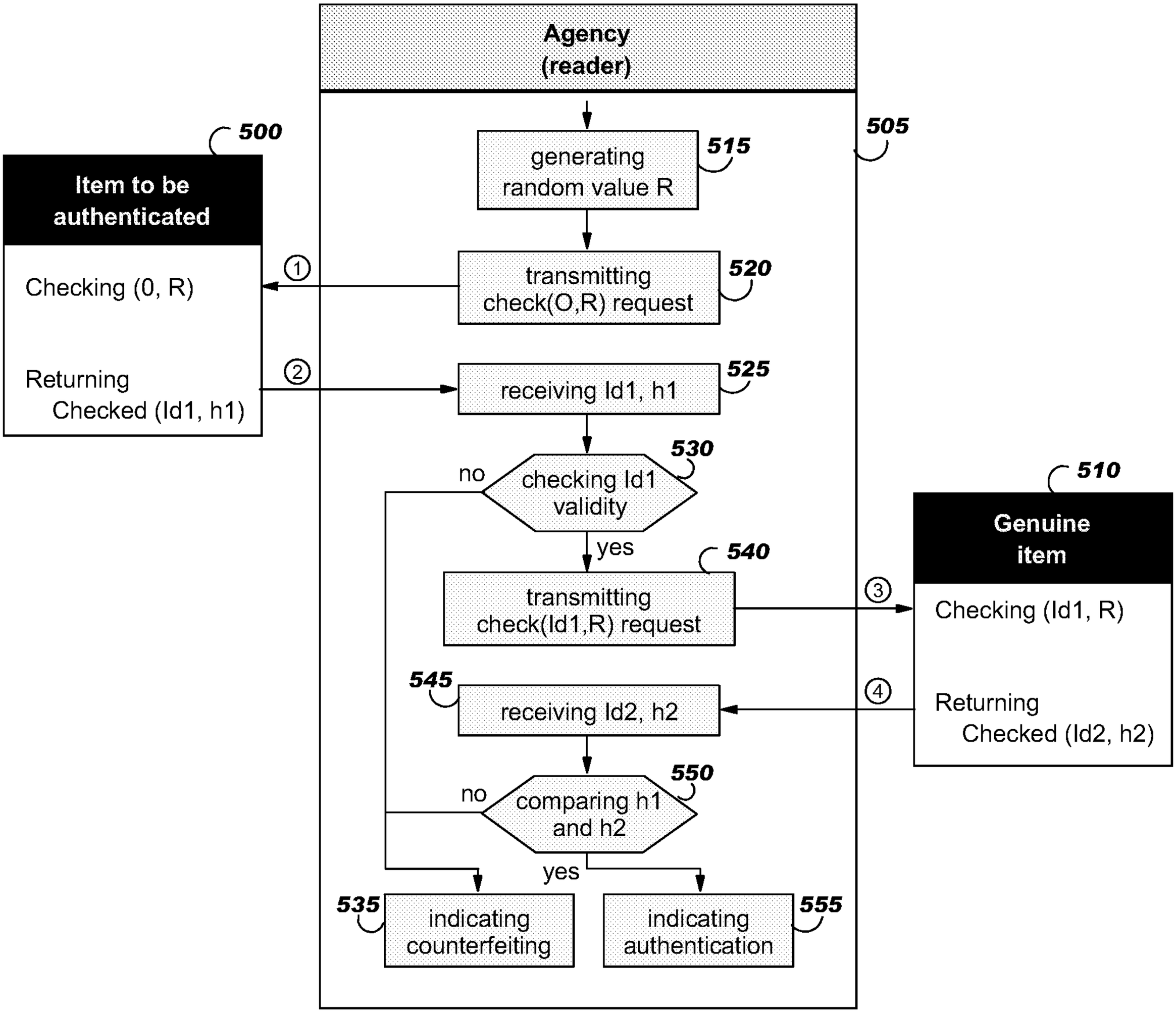


Figure 6


Agency
(reader)
505
500
Item to be authenticated
Checking (0, R)
Returning Checked (Id1, h1)
generating random value R
515
transmitting check(O,R) request
520
receiving Id1, h1
525
checking Id1 validity
530
no
yes
transmitting check(Id1,R) request
540
receiving Id2, h2
545
comparing h1 and h2
550
no
yes
indicating counterfeiting
535
indicating authentication
555
510
Genuine item
Checking (Id1, R)
Returning Checked (Id2, h2)
1
2
3
4