



166166

1

15 NOV 2005

METHOD TO ADDRESS SECURITY AND PRIVACY ISSUES OF THE USE OF RFID SYSTEMS TO TRACK CONSUMER PRODUCTS

BACKGROUND OF THE INVENTION

1. Technical Field:

The present invention relates generally to the area of identification devices. More particularly, the present invention provides a radio-frequency identification system with features to reduce a party's ability to tamper with the identification devices or to track the identification devices on a global scale. The invention is particularly useful as a theft/fraud preventive in the context of a retail store or as a means of inventory control when accuracy is critical, such as with an inventory of pharmaceuticals in a clinical setting.

2. Description of Related Art:

Radio-frequency identification (RFID) technology provides an inexpensive and simple way to mark physical objects with machine-readable information. In this application, the term "machine-readable" refers to those media that are readable only by a machine; such media are almost always machine written as well. RFID has many advantages over other machine-readable information media. Unlike magnetic media, RFID tags do not require a reader to make contact with the tag to read the information out. Unlike bar codes, RFID tags can be easily rewritten and do not require that the tag be visible when read.



G00002

RFID tags are electronic devices. They are generally composed of an antenna and an integrated circuit. The antenna is used for sending and receiving data as radio-frequency signals. The integrated circuit contains non-volatile memory, modulation circuitry (for facilitating radio communication), and control logic. Thus, RFID tags are memory devices that are read and written to using radio-frequency signals.

RFID tags are passive devices. That means that they need not include a power supply. RFID tags receive all the power they need to operate from the radio-frequency signal emitted by RFID tag readers or writers. This makes it possible to manufacture RFID tags of very small size. Advancements in RFID tag fabrication technology have also made it possible for RFID tags to be manufactured at very small sizes. For instance, early RFID tags used large inductive antennas; more modern tags use capacitive antennas, which can be printed on packaging using conductive ink in a way that blends in with other printed marking. With this new antenna manufacturing technique the integrated circuit can simply be glued on to the antenna looking, perhaps, like just a "dot" in the product logo or other printing.

RFID tags, because of their small size, are easily incorporated into other products. For instance, RFID tags can be easily sewn into clothes or attached to product packaging, or incorporated into product markings. This makes them prime candidates for storing product information, such as universal product codes (UPCs) or

price information, in a retail product, much as bar codes do for supermarket products today.

Another use for RFID tags, one that has already gained wide acceptance, is to use RFID tags as a theft detection system. In such a system, RFID-tagged merchandise, when transported past a reader device in front of the exit to a store, triggers an alarm, unless the tag has been reprogrammed at the point-of-sale when the item is purchased.

Three problems with the widespread use of RFID tags on merchandise occur, however. The first is that many current RFID tags can be readily tampered with. Current RFID tags generally impose no access control requirements and may be read from and written to freely. Thus, a store employee with less than honorable intentions might reprogram the tag on a particular piece of merchandise such that when the employee buys the merchandise from the store, the employee is undercharged.

The second problem is one that also occurs with some frequency with bar codes. Sometimes the point-of-sale terminal at which an item is being purchased is programmed with incorrect price information. This situation can result in the customer being overcharged or even undercharged. Because the RFID tag is machine-readable only, it provides no price information to the cashier. Thus, there is often no way for the cashier to detect a mistake in a customer's receipt.

The third problem is that the widespread use of RFID tags on merchandise such as clothing would make it possible for the locations of people, animals, and

objects to be tracked on a global scale—a privacy invasion of Orwellian proportions.

SUMMARY OF THE INVENTION

Accordingly, it would be beneficial if there were a method of storing product information in a radio-frequency identification tag attached to the product in such a way as to avoid the problems associated with tampering of tags. It would also be desirable to avoid the problems associated with the tracking of RFID tags on a global scale. It would also be desirable to implement an RFID system that protects against pricing errors at the point-of-sale.

The present invention achieves these goals by employing a novel method for managing the storage of product information in an RFID tag. In a preferred embodiment of the invention, product information is divided into three categories: a universal product code (UPC), a list price, and a tracking number. Each of these categories is stored as a triplet. The triplet includes a type (which denotes an access control rule associated with the category), a value (containing the primary information stored in the category), and a length (of the value).

The UPC and list price categories are stored as read-only-type data, to prevent tampering, and the tracking number is stored under a "short-update" type. The short update type allows a globally-unique tracking number used for inventory purposes to be overwritten with a globally non-unique number at the point-of-sale to prevent global tracking. Finally, point-of-sale pricing

mistakes are easily detected by comparing the read-only list price stored in the RFID tag with the price stored in the point-of-sale terminal. If the two prices are widely divergent, then the attending cashier is alerted to the discrepancy.

Broadly, the invention provides a method for secure electronic labeling, the method comprising the steps of:

- (a) writing a value to a first memory having a length, the first memory being part of a machine-readable identification device that is part of an electronic label;
- (b) writing a type to a second memory in the machine-readable identification device wherein the type written to the second memory identifies a type of access control rule that is to control overwriting the value written to the first memory; and
- (c) responsive to steps (a) and (b), imposing a first access control rule upon the first memory based on the type written to the second memory.

The invention further provides a computer program product, in a computer-readable medium, for secure electronic labeling, the computer program product comprising instructions for:

- (a) writing a value to a first memory having a length, the first memory being part of a machine-readable identification device that is part of an electronic label;
- (b) writing a type to a second memory in the machine-readable identification device, wherein the type written to the second memory identifies a type of access control rule that is to control overwriting the value written to the first memory; and
- (c) responsive to the instructions for (b) and (c), imposing a first access control rule upon the first memory based on the type written to the second memory.

The invention yet further provides an apparatus for secure electronic labeling, comprising:

- a communication unit;
- a controller, configured to receive data from the communication unit;
- a memory, having a length, and configured to be written to by the controller,

wherein the communication unit receives a value, the controller receives the value from the communication unit, the controller evaluates an access control rule taken from a plurality of access control rules to determine whether the value should be written to the memory, and if the controller determines that the value should be written to the memory, the controller writes the value to the memory, wherein the communication unit, controller, and memory are part of a same electronic label.

BRIEF DESCRIPTION OF THE DRAWINGS

The novel features believed characteristic of the invention are set forth in the appended claims. The invention itself, however, as well as a preferred mode of use, further objectives and advantages thereof, will best be understood by reference to the following detailed description of an illustrative embodiment when read in conjunction with the accompanying drawings, wherein:

Figure 1 depicts a typical radio-frequency identification (RFID) tag.

Figure 2 depicts common physical embodiments and applications of RFID technology.

Figure 3 depicts, in storyboard format, the use of the present invention's RFID technology in a retail context.

Figure 4A is a diagram depicting the memory contents of a preferred embodiment of the present invention.

Figure 4B is a diagram depicting the modified memory contents of a preferred embodiment of the present invention.

Figure 4C is a diagram depicting how a short-update write-access control rule allows for local tracking, but prevents global tracking.

Figure 5 is a block diagram of a preferred embodiment of the present invention.

Figure 6 is a C language representation of the process of writing information to an RFID tag of the present invention.

Figure 7 is a C language representation of the process of reading information from an RFID tag of the present invention.

Figure 8 is a flowchart depicting the process of writing information to an RFID tag of the present invention.

Figure 9 is a flowchart depicting the process of adding an RFID-tagged item to a customer's order, in accordance with a preferred embodiment of the present invention.

Figure 10 is a flowchart depicting the process of theft/fraud detection in accordance with a preferred embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Figure 1 is an example of a radio-frequency identification (RFID) tag 100 (not to scale). The tag 100 includes an integrated circuit 110 containing non-volatile memory, logic circuitry, and communications circuitry. This integrated circuit is attached to an antenna 120, which in this example is implemented as an inductor coil. All of this electronic equipment is fabricated onto a substrate, which in this example is a clear, flexible film.

This tag 100 may be written to or read from by subjecting it to a radio-frequency signal. The integrated circuit 110 reads the radio-frequency signal from the antenna 120 and interprets the signal as a command to read or write data to or from memory located on the integrated circuit.

Note that there is no power supply located on the tag 100. The integrated circuit 110 collects all of its power from the energy in the radio-frequency signal. This allows the tags to be easily and inexpensively produced and allows them to be used in a variety of environments where a device that had to supply its own power could not be used. An example of such an environment would be one in which the bulk of a power supply would be prohibitive.

RFID tags provide a ready form of identification or marking of an object. Identification information can be written to an RFID tag, where it becomes readable by any

compatible reader. The kinds of information that may be stored in an RFID tag are essentially all of the same kinds of information that may be stored in a computer or other data processing system. Thus, an RFID tag identifying an item of merchandise, for instance, may include such information as the name of the product, price information, a serial number, a UPC (Universal Product Code), or any other data a merchant or manufacturer may choose to include.

As **Figure 2** demonstrates, RFID technology can take many forms and be used in many contexts. A tag 100, such as the one in **Figure 1** is readily mounted to or incorporated into a variety of products. A tag 100 may be mounted to an item of product packaging 210 or placed within the pages of a book 200.

Although not tags in the usual sense of the word, a number of access control and identification devices that do not resemble the flat tag also fall into the same category. Among these are the RFID key fob 230, which is an RFID tag that is attached to a key ring 240, and the RFID card 250, which is often used as an access control device in parking garages or other restricted areas.

These examples are not intended to be exhaustive of the applications or forms of RFID tags. Many other applications and physical forms of the technology are known to exist or are being developed.

Figure 3 shows, in a storyboard format, a high level overview of how the present invention uses RFID tags in a retail context. In the first frame 305, a retail customer 300 selects a product 310, in this case a coat,

to which an RFID tag is attached. The RFID is preferably attached to the product in such a way as to prevent an unsuspecting customer or a would-be shoplifter from finding and removing the tag. In the case of a coat, the tag could be sewn into the lining, for instance.

In the second frame 325, the customer 300 brings the product 310 to a point-of-sale terminal 315. The attending cashier 320 scans the product 310 with a tag reader/writer 330. The tag reader/writer 330 reads a product identification code (such as a UPC) and an inventory tracking code from the tag attached to the product 310. The point-of-sale terminal 315 then adds the product 310 to the customer's 300 order and overwrites the tracking information with the tag reader/writer 330 so as to signify that the product 310 has been purchased.

In the third frame 335, when the customer 300 leaves the store with the customer's 310 tagged items of merchandise 340, RFID readers 350 placed in front of the exit 360 scan the tagged items 340 to ensure that they have been paid for. If the customer's items 340 were not paid for (in other words, if they retain their original tracking numbers), a theft alarm 370 is sounded.

Figure 4A is a diagram of the memory contents of an RFID tag attached to a product 310 as in Figure 3, in accordance with a preferred embodiment of the present invention. Three basic pieces of information are stored in the tag. These are represented by rows 400 in the diagram. The UPC 402 identifies which product (among differing products) is attached to the tag. The list

price 404 gives an indication of the manufacturer's or retailer's suggested retail price for the item; this allows a point-of-sale terminal to detect gross errors in its pricing information by comparing its information to the list price, thus preventing a customer being mistakenly over- or under-charged for an item. The tracking number 406 uniquely identifies the particular item of merchandise attached to the tag as among other items in the store or as among other items on a global scale (all items of merchandise in the world, for instance).

Each of the three pieces of information is represented as a triplet comprising a type 412, a length 414, and a value 416. The type field 412 indicates to what extent the information stored on the tag may be changed. For instance, the UPC 402 is stored on the tag in **Figure 4A** using the read-only 420 type. That means that the UPC 402 cannot be changed. Storing the UPC 402 as a read-only value keeps a would-be con artist (such as a retail employee with criminal leanings) from changing a product's UPC 402 to that of a less expensive product, so as to be charged less at the point-of-sale terminal 315 (in **Figure 3**). Other possible types include unlimited read/write and short rewrite, which will be discussed later in regard to **Figure 4B**.

The length field 410 denotes how long the information stored in the value field 416 may be. For instance, in **Figure 4A**, the UPC length field 422 limits the size of the UPC value field 424 to 10 bytes.

In **Figure 4A**, the tracking number 406 is stored with short-rewrite 430 type. This means that if an attempt to rewrite the tracking number value 433 is made, the tracking number length 432 is shortened to some predetermined length, and only a new tracking number of length equal to the predetermined length will be stored.

Figure 4B demonstrates what happens to the memory when a short-rewrite type data field is rewritten to. In **Figure 4B**, the tracking number length 432 has been shortened to three bytes, and a value of no more than three bytes length has been stored as the tracking number value 433. Here, it is the date and order of sale (the thirty-sixth sale on January 30, 2001). Limiting the size of the rewritten information provides protection to the customer against global tracking.

Figure 4C demonstrates how this protection against global tracking works. When a customer 450 is located within a store 460 and is carrying something storing a small tracking number containing largely non-unique information (such as a date, along with a few digits of tracking number), that customer's 450 location may be tracked throughout the store. Even though the amount of tracking information may be small, because there are few others within the store, there is little likelihood that two customers having the same number are in the same store. Thus, the customer 450 can be uniquely identified and readily tracked.

A customer 470 who has left the store holding a small tracking number, however, is not easily distinguishable from the rest of the population. If the

customer's 470 tracking number is limited in size, there will be (many) others with the same tracking number. Thus, it will become difficult to uniquely identify and track the customer 470.

Figure 5 is a block diagram of a preferred physical embodiment 500 of the RFID tags of the present invention. An antenna 510 receives a radio-frequency signal from a tag-reading or tag-writing device. The signal passes to a demodulator circuit 520, which separates the information-bearing component of the signal from a carrier signal. Decode circuitry 530 converts the output of the demodulator 520 into digital data and instructions that the control logic 540 can understand.

The control logic 540 interprets the instructions given to it to either read or write to/from the value memory 560, which stores the identification information (UPC, list price, etc.) and the length of each element of such information. The control logic 540, is governed, however, by the contents of the type memory 550, which stores the contents of the type field 412, found in **Figure 4A**.

Thus, when attempting to write a data to a location in value memory 560, the control logic 540 first checks the type memory 550 to see if the data may be written to the location and if so, how much data may be written there. If the location may be written to, the data and the proper length are stored in the value memory 560.

When an item of data is read, the control logic 540 first reads the length of the data item from the value memory 560, then reads that length of data from the value

memory 560. The control logic 540 then sends that data to encode circuitry 570, which converts the data into a form suitable for transmission over a radio-frequency communications channel. The converted data then passes to a modulator 580, which modulates a carrier signal to include the converted data. The modulated signal is then transmitted as radio waves through the antenna 510.

Figure 6 shows a C language representation 600 of the process of writing a record to memory within an RFID tag of a preferred embodiment of the present invention. Those skilled in the art will appreciate that this representation is only an example of how the control logic 540 of Figure 5 can be implemented in software, using a microcontroller, microprocessor, or digital signal processor as the physical embodiment of the control logic 540. Those skilled in the art will also appreciate that such a software implementation is not limited to the use of the C language but may be implemented in any of a variety of computer languages, including but not limited to C++, Java, Forth, Lisp, Scheme, Python, Perl, and Assembly Languages of all kinds. Further, those skilled in the art will recognize that the control logic 540 need not be implemented as software running on a microcontroller, microprocessor, digital signal processor, or other stored-program data processing device; the control logic 540 may as easily be implemented using application-specific circuitry (such as digital logic circuitry) with no stored program of instructions.

Figure 6 demonstrates an alternative embodiment of the invention in which the "type" portion of a data triplet stores the category of information (UPC, price, etc.) being stored, rather than the write-access rule (read-only, short-rewrite, etc.). In this embodiment, the write access rules are associated with each category of information (UPCs are read-only, tracking numbers are short-rewrite, etc.). Thus, whereas in the previous figures, the type field denoted the write access rule explicitly, the type field in **Figure 6** denotes the write access rule implicitly, as a result of the association between each data category and an access control rule.

In the C language representation **600**, the data triplets (type, length, value) are stored together in a struct data structure **610**. The type **615** is stored as a character string. The length **630** is stored as an integer, and the value is stored as an array of bytes (chars) **640**.

The data triplets are stored in the memory of the RFID tag. In **Figure 6**, that memory is organized by using an array of pointers to data triplets (structs) **642**. Each element in the array is a pointer that points to a data triplet stored in a struct.

The writing process is embodied in the function "write_record" **650**. A data triplet struct **652** is passed into the function **650**. The struct **652** contains the new information to be written, the length of the information, and the desired type to associate with the information. The function **650** defines two variables: a pointer that will point to an existing struct of the same type ("old")

656 and a variable 620 for storing the write access control rule associated with the existing struct 656.

The execution of the function 650 is as follows: In line 657, an existing struct of the same type as the new information 652 is searched for in memory using a function "findItemByType" (not listed). In line 658, if no such existing struct is found, a function called "addNewType" (not listed) is called to make a new struct of the new type. The existing struct or new struct, accordingly, is pointed to by variable "old" 656.

In line 659, the write access control rule governing the type of the struct pointed to by "old" 656 is found and stored in "old_rule" 620. In line 660, if "old_rule" 620 is "read_only" 622, then exit the function, as the struct pointed to by "old" 656, being of read-only type, may not be written to. In line 670, if "old_rule" is "short_rewrite," then a predetermined length, MAXLEN, is substituted for the length stored in the struct pointed to by "old" 656. MAXLEN is defined in this example to be three bytes, per line 675. In line 680, if "old_rule" is "read_write," then the entirety of the data stored in the passed-in struct 652 may be stored in the struct pointed to by "old" 656; thus the length stored in the struct pointed to by "old" 656 is adjusted to the length 654 the information to be stored.

Finally, in line 690, the data portion of the passed-in struct 652 is copied into the value array 640 of the struct 656.

Figure 7 depicts a C language function "read_record" 700 for reading values from the RFID tag. A counted loop

720 is set up to iterate through each data triplet struct in memory. Each iteration through the loop, the type 730, length 740, and data contents 750 are transmitted.

Figure 8 is a flowchart representation of the process the control logic 540 goes through in writing an item of data to the memory of an RFID tag in a preferred embodiment of the present invention. First the instruction to write a particular item of data to a particular location within the memory is received (step 800). If the location in question is a read-only location (step 810), the process ends (step 820), since no data is allowed to be written. If not, however, the control logic 540 must then check to see if the location is governed by a short-rewrite rule (step 830). If it is, then the length associated with the memory location is shortened (step 840), pursuant to the short-rewrite rule. If not, then the length associated with the memory location is adjusted to fit the new item of data (step 850). Finally, as much of the new item of data as will fit, given whichever length adjustment is performed (step 840 or step 850), is written to the memory location (step 860).

Figure 9 is a flowchart representation of the process a point-of-sale terminal would follow in adding a tagged item to the customer's order, in a preferred embodiment of the invention. First, the RFID tag is read to obtain the UPC and list price of the tagged item (step 900). Next, the actual retail price of the item is looked up in a database by using the UPC as a search key (step 910). If the price looked up from the database is

sufficiently close to the list price stored on the tag (step 920), the item is added to the customer's sales receipt (step 940) and the customer is charged for the item. If the two prices are sufficiently different (step 920), the cashier is notified to alert a manager to the discrepancy (step 930), so that the customer is not overcharged for the item, for instance.

Figure 10 is a flowchart representation of the process the theft-detection portion of a preferred embodiment of the invention would follow in detecting theft or fraud. First the tracking number 406 (in Figure 4A) is read from the RFID tag on a tagged item of merchandise (step 1000). This would normally occur using reader 350 placed before the exit 360 of a store (see Figure 3). If the tracking number 406 has been given a short length (step 1010), this means that the item has had its tracking number overwritten (most likely because the item has been purchased). But if it has not, the item has not been purchased, and theft is detected (step 1020).

If the tracking number 406 has been given a short length (step 1010), then the tracking number 406 is compared with either store records or against the value stored in an RFID tag affixed to the customer's receipt, or both (step 1030). If they do not match, then the tagged item has had its tag tampered with, and store personnel are notified (step 1040).

A number of variations on the basic invention disclosed here have been contemplated. Possible variations include, but are not limited to the following.

The invention is not limited to using radio-frequency signals. Any kind of electromagnetic radiation, including visible and invisible light, could be used as a communications medium. In addition, sound waves (at an ultrasonic frequency, for instance) could also be used as a communications medium.

The physical embodiment of the invention is not limited to the use of electronic circuitry. For instance, research is currently being conducted in the area of optical computing components as a speedier alternative to electronic components. The present invention is applicable to such technology or to any other physical data processing technology that may be developed.

The physical embodiment is not limited to the use of monolithic semiconductor chip technology. Research is being conducted in the area of chipless RFID devices. The present invention is applicable to chipless RFID technology as well as to RFID devices utilizing a semiconductor chip.

The present invention could also include an ability for specially authorized users to manually modify the type and length information on an RFID tag. This would allow an organization with sufficient authority, like a retailer or manufacturer, the ability to reset a tag to its pre-purchase state. Many authentication and cryptographic schemes, such as secret sharing and various handshaking protocols, exist in the prior art to allow an authorized party access without compromising security. This feature would be useful for handling returned

merchandise in a retail context, where tags need to be reset before the merchandise is returned to the retail floor.

The present invention is not limited to the retail context. Indeed, the basic goals of the present invention, namely protection against data tampering and against global tracking, are applicable in a number of contexts outside of the retail sector. For instance, the same technology could as easily be utilized in the context of a circulating library, where books are tagged with RFID tags. Information regarding the identity and ownership of a volume can be stored as read-only information and information about the book's circulation can be stored in a short-rewrite field that is reset to its pre-checkout length and value when returned to the library.

Another use for the present invention is for keeping track of a pharmaceutical inventory in a clinical setting. In a hospital or clinic, it is crucial that drugs are administered in the proper amounts, and that the hospital or clinic has an accurate assessment of their drug inventory at all times. By tagging pharmaceutical products with RFID tags in accordance with the present invention, a health care facility can ensure that accurate information regarding the inventory and usage of pharmaceutical products is maintained at all times.

It is important to note that while the present invention has been described in the context of a fully functional data processing system, those of ordinary

skill in the art will appreciate that the processes of the present invention are capable of being distributed in the form of a computer readable medium of instructions and a variety of forms and that the present invention applies equally regardless of the particular type of signal bearing media actually used to carry out the distribution. Examples of computer readable media include recordable-type media such a floppy disc, a hard disk drive, a RAM, and CD-ROMs and transmission-type media such as digital and analog communications links.

The description of the present invention has been presented for purposes of illustration and description, but is not intended to be exhaustive or limited to the invention in the form disclosed. Many modifications and variations will be apparent to those of ordinary skill in the art. The embodiment was chosen and described in order to best explain the principles of the invention, the practical application, and to enable others of ordinary skill in the art to understand the invention for various embodiments with various modifications as are suited to the particular use contemplated.

CLAIMS:

1. A method for secure electronic labeling, the method comprising the steps of:
 - (a) writing a value to a first memory having a length, the first memory being part of a machine-readable identification device that is part of an electronic label;
 - (b) writing a type to a second memory in the machine-readable identification device wherein the type written to the second memory identifies a type of access control rule that is to control overwriting the value written to the first memory; and
 - (c) responsive to steps (a) and (b), imposing a first access control rule upon the first memory based on the type written to the second memory.
2. A method for secure electronic labeling, the method comprising the steps of:
 - (a) writing a value to a first memory having a length, the first memory being part of a machine-readable identification device;
 - (b) writing a type to a second memory in the machine-readable identification device; and
 - (c) responsive to steps (a) and (b), imposing a first access control rule upon the first memory, wherein the first access control rule is that if the first memory is rewritten to, the length of the first memory is reduced to a predetermined size.
3. The method of claim 1, wherein the machine-readable identification device comprises a radio-frequency identification (RFID) tag.
4. The method of claim 3, wherein the first access control rule is that the first memory may not be rewritten.

5. The method of claim 3, comprising the step of (d) selecting the first access control rule from a plurality of access control rules.

6. A method for secure electronic labeling, the method comprising the steps of:

- (a) writing a value to a first memory having a length;
- (b) writing a type to a second memory;
- (c) reading a request to overwrite the first memory;
- (d) responsive to step (c), if the type is of a first kind, disallowing overwriting of the first memory;
- (e) responsive to step (c), if the type is of a second kind, overwriting the first memory and shortening the length of the first memory;
- (f) responsive to step (c), if the type is of a third kind, overwriting the first memory with new data and adjusting the length of the first memory to fit the new data.

7. The method of claim 6, wherein in step (e) the length of the first memory is shortened to a predetermined size.

8. A method for secure electronic labeling, the method comprising the steps of:

- (a) writing a value to a first memory having a length, the first memory being part of a

machine-readable identification device that is part of an electronic label;

(b) associating a type value with the first memory such that an access control rule is imposed upon the first memory, in accordance with the type value, wherein the access control rule controls overwriting of the value written to the first memory.

9. A method for secure electronic labeling, the method comprising the steps of:

(a) writing a value to a first memory having a length, the first memory being part of a machine-readable identification device;

(b) associating a type value with the first memory such that an access control rule is imposed upon the first memory, in accordance with the type value, wherein the access control rule is such that if the first memory is rewritten to, the length of the first memory is reduced to a predetermined size.

10. The method of claim 9, wherein step (b) is executed in response to an execution of step (a).

11. The method of claim 8, wherein the machine-readable identification device is a radio-frequency identification (RFID) tag.

12. The method of claim 11, wherein the access control rule is such that the first memory may not be rewritten to.

13. A computer program product, in a computer-readable medium, for secure electronic labeling, the computer program product comprising instructions for:

(a) writing a value to a first memory having a length, the first memory being part of a machine-readable identification device that is part of an electronic label;

(b) writing a type to a second memory in the machine-readable identification device, wherein the type written to the second memory identifies a type of access control rule that is to control overwriting the value written to the first memory; and

(c) responsive to the instructions for (b) and (c), imposing a first access control rule upon the first memory based on the type written to the second memory.

14. A computer program product, in a computer-readable medium, for secure electronic labeling, the computer program product comprising instructions for:
- (a) writing a value to a first memory having a length, the first memory being part of a machine-readable identification device;
 - (b) writing a type to a second memory in the machine-readable identification device; and
 - (c) responsive to the instructions for (b) and (c), imposing a first access control rule upon the first memory, wherein the first access control rule is that if the first memory is rewritten to, the length of the first memory is reduced to a predetermined size.
15. The computer program product of claim 13, wherein the machine-readable identification device is a radio-frequency identification (RFID) tag.
16. The computer program product of claim 15, wherein the first access control rule is that the first memory may not be rewritten to.
17. The computer program product of claim 15, comprising instructions for (d) selecting the first access control rule from a plurality of access control rules.
18. A computer program product, in a computer-readable medium, for secure electronic labeling, the method comprising instructions for:
- (a) writing a value to a first memory having a length;
 - (b) writing a type to a second memory;
 - (c) reading a request to overwrite the first memory;

- 27 -

(d) responsive to the instructions for (c), if the type is of a first kind, disallowing overwriting of the first memory;

(e) responsive to the instructions for (c), if the type is of a second kind, overwriting the first memory and shortening the length of the first memory;

(f) responsive to the instructions for (c), if the type is of a third kind, overwriting the first memory with new data and adjusting the length of the first memory to fit the new data.

19. The computer program product of claim 18, wherein in the instructions for (e), the length of the first memory is shortened to a predetermined size.

20. A computer program product, in a computer-readable medium, for secure electronic labeling, comprising instructions for:

(a) writing a value to a first memory having a length, the first memory being part of a machine-readable identification device that is part of an electronic label;

(b) associating a type value with the first memory such that an access control rule is imposed upon the first memory, in accordance with the type value, wherein the access control rule controls overwriting of the value written to the first memory.

21. A computer program product, in a computer-readable medium, for secure electronic labeling, comprising instructions for:
- (a) writing a value to a first memory having a length, the first memory being part of a machine-readable identification device;
 - (b) associating a type value with the first memory such that an access control rule is imposed upon the first memory, in accordance with the type value, wherein the access control rule is such that if the first memory is rewritten to, the length of the first memory is reduced to a predetermined size.
22. The computer program product of claim 21, wherein the instructions for (b) are executed in response to an execution of the instructions for (a).
23. The computer program product of claim 20, wherein the machine-readable identification device is a radio-frequency identification (RFID) tag.
24. The computer program product of claim 23, wherein the access control rule is such that the first memory may not be rewritten to.
25. An apparatus for secure electronic labeling, comprising:
- a communication unit;
 - a controller, configured to receive data from the communication unit;
 - a memory, having a length, and configured to be written to by the controller,
- wherein the communication unit receives a value, the controller receives the value from the communication unit, the controller evaluates an access control rule taken from a plurality of access control rules to determine whether the value should be written

- 29 -

to the memory, and if the controller determines that the value should be written to the memory, the controller writes the value to the memory, wherein the communication unit, controller, and memory are part of a same electronic label.

26. The apparatus of claim 25, wherein the access control rule is such that the value is written to memory, but the length of the memory is reduced to a predetermined size.
27. The apparatus of claim 26, comprising an integrated circuit, wherein the memory is formed using the integrated circuit.
28. The apparatus of claim 26, comprising an integrated circuit, wherein the controller is formed using the integrated circuit.
29. The apparatus of claim 26, comprising an integrated circuit, wherein the communication unit is formed using the integrated circuit.
30. The apparatus of claim 26, wherein the apparatus is attached to a substrate.
31. The apparatus of claim 30, wherein the substrate is a flexible sheet material.
32. The apparatus of claim 30, wherein the substrate is an article of merchandise.

33. The apparatus of claim 30, wherein the substrate is an item of packaging.

34. The apparatus of claim 26, wherein the communication unit receives the value as an electromagnetic stimulus.

35. The apparatus of claim 34, wherein the electromagnetic stimulus comprises light.

36. The apparatus of claim 34, wherein the electromagnetic stimulus comprises radio waves.

37. The apparatus of claim 34, comprising a photoelectric cell, wherein the communication unit receives the value as an electromagnetic stimulus through the photoelectric cell.

38. The apparatus of claim 34, comprising an antenna, wherein the communication unit receives the value as an electromagnetic stimulus through the antenna.

39. The apparatus of claim 38, wherein the antenna comprises a capacitive antenna.

40. The apparatus of claim 26, wherein the predetermined size is three bytes.

41. The apparatus of claim 26, wherein the access control rule is stored in a second memory.

42. The apparatus of claim 26, wherein the access control rule is embodied in a logic circuit.

43. The apparatus of claim 26, wherein the memory is configured to be read by the controller, and the communication unit is configured to receive data from the controller, and wherein the controller reads the value from the memory, the communication unit receives the value from the controller, and the communication unit transmits the value.

44. The apparatus of claim 43, wherein the communication unit transmits the value as electromagnetic radiation.

45. The apparatus of claim 44, wherein the electromagnetic radiation comprises light.

46. The apparatus of claim 44, wherein the electromagnetic radiation comprises radio waves.

47. The apparatus of claim 25, wherein the access control rule is such that once the value is written to the memory, the memory may not be rewritten to.

48. The apparatus of claim 47, comprising an integrated circuit, wherein the memory is formed using the integrated circuit.

49. The apparatus of claim 26, comprising an integrated circuit, wherein the controller is formed using the integrated circuit.

50. The apparatus of claim 26, comprising an integrated circuit, wherein the communication unit is formed using the integrated circuit.

51. The apparatus of claim 47, wherein the apparatus is attached to a substrate.

52. The apparatus of claim 51, wherein the substrate is a flexible sheet material.

53. The apparatus of claim 51, wherein the substrate is an article of merchandise.

54. The apparatus of claim 51, wherein the substrate is an item of packaging.

55. The apparatus of claim 47, wherein the communication unit receives the value as an electromagnetic stimulus.

56. The apparatus of claim 55, wherein the electromagnetic stimulus comprises light.

57. The apparatus of claim 55, wherein the electromagnetic stimulus comprises radio waves.

58. The apparatus of claim 55, comprising a photoelectric cell, wherein the communication unit receives the value as an electromagnetic stimulus through the photoelectric cell.

59. The apparatus of claim 55, comprising an antenna, wherein the communication unit receives the value as an electromagnetic stimulus through the antenna.

60. The apparatus of claim 59, wherein the antenna comprises a capacitive antenna.

61. The apparatus of claim 47, wherein the access control rule is stored in a second memory.

62. The apparatus of claim 47, wherein the access control rule is embodied in a logic circuit.

63. The apparatus of claim 47, wherein the memory is configured to be read by the controller, and the communication unit is configured to receive data from the controller, and wherein the controller reads the value from the memory, the communication unit receives the value from the controller, and the communication unit transmits the value.

64. The apparatus of claim 63, wherein the communication unit transmits the value as electromagnetic radiation.
65. The apparatus of claim 64, wherein the electromagnetic radiation comprises light.
66. The apparatus of claim 64, wherein the electromagnetic radiation comprises radio waves.
67. A system for inventory control, the system comprising:
an item, wherein the item is tagged with a machine-readable tag, and the machine-readable tag stores a tracking number, wherein the machine-readable tag stores a length associated with the tracking number;
a reader for reading the machine-readable tag;
a writer for writing the machine-readable tag; and
a data processing system in communication with the reader and the writer, wherein the reader reads the tracking number from the tag, the data processing system stores the tracking number, the writer shortens the length, and the writer writes a new tracking number to the machine-readable tag.
68. The system of claim 67, wherein the machine-readable tag comprises a radio-frequency identification (RFID) tag.
69. The system of claim 67, wherein the data processing system is a point-of-sale terminal.
70. The system of claim 67, wherein the writer authenticates itself to the machine-readable tag before writing to the machine-readable tag.
71. The system of claim 67, comprising a second reader positioned in front of an exit, wherein if the machine-readable tag is read by the second reader and the machine-readable

- 35 -

tag has not had the length of the tracking number shortened, the second reader triggers a theft alarm.

72. The system of claim 67, comprising a plurality of secondary readers, wherein the plurality of secondary readers track movement of the item throughout a geographic area.

73. The system of claim 67, wherein the item is a pharmaceutical product.

74. The system of claim 73, comprising a plurality of secondary readers, wherein the plurality of secondary readers track movement of the item throughout a health-care facility.