# Privacy Enhanced Authentication Protocol for RFID Tag System Security

**Sang-Soo Yeo**[†] **and Jin Kwak**[††],

[†]Dept. of Computer Science & Communication Engineering,
Kyushu University, Japan
[††]Dept. of Information Security Engineering,
Soonchunhyang University, Korea.

**Summary**
Radio Frequency Identification (RFID) system is now becoming widely accepted for many ubiquitous computing applications. However, RFID system has some privacy problems. Therefore, many researches results related to security and privacy in RFID system. However, we cannot choose anything among them for applying to the current RFID system. Most of them require either of high-cost hardware specification or giving up potential convenience of consumers. In this paper, we propose a simple privacy protection scheme that can be used for the current existing RFID system such as ISO 18000-6 type C. We modify this standard tag identification protocol slightly and introduce a light-weight proxy device for privacy enhancing.
.

***Key words:***
*RFID system, authentication, privacy, security.*

## 1. Introduction

The main technology of the ubiquitous computing application is RFID system that recognizes and manages RFID tag through the RF (Radio Frequency) signal. Low-cost RFID tags can be read, and information can be updated without physical contact. Therefore, RFID system has become popular for automated identification in the ubiquitous computing applications[15, 16].

Furthermore, we expect that RFID technology will be the next one of the bar-code system in the area of automatic identification. It will be not only substitutes of the existing bar-code applications, but also pioneers of new creative services such as speedy checkouts in the shops, receiptless item returns, recycling, pets identification, more user-dependent services. For dreams come true, we need to solve some problems, which are reducing manufacturing and packaging costs, lowering tag's power consumption, standardization, security, and privacy problems. Thus, several methods of protecting the users' location privacy have been proposed [2-4, 8]. Now we have to focus on its privacy problems for RFID system's popularization [1, 2].

Normally a tag emits its unique identifier to any reader without any authentication phase. This characteristic is the origin of security and privacy problems in RFID system. In the near future, that may be equipped by RFID, at any time the user will be able to know easily what kind of man someone is, just using user's RFID reader to scan his items [1-8]. Anyone who has lots of readers and a logging system will be able to retrieve location histories of us from his system [3-9].

In this paper, we will address some of the existing security schemes related to privacy protection and also introduce the singulation protocol of ISO 18000-6 Type C before describing our scheme [10].

## 2. RFID System Overview

### 2.1 EPC

The binary representation of the EPC (Electronic Product Code), a combination of *Header*, *EPC Manager*, *Object Class*, and *Serial Number*. *Header* identifies the version, length, tag type, and structure of the code. *EPC Manager* identifies a company, a manager, or an organization. In short, it indicates a manufacturer ID. *Object Class* indicates article classification (manufacturer's product ID). The class number must be unique for all given domains. *Serial Number* is unique for every class and non-repeating for each object class code.

The figure 1 shows the EPC and figure 2 shows EPC network.

- ***Header*** : identifies the version, length, tag type, and structure of the code. The 64-bit type assigns 2-bit for the header field, whereas 96/256-bit types use an 8-bit header.
- ***EPC Manager*** : identifies a company, a manager, or an organization. This value ensures that each domain

[††]Prof. Jin Kwak, he is corresponding Author of this paper, (jkwak@sch.ac.kr)

Manuscript received September 5, 2007
Manuscript revised September 20, 2007

number is unique. In short, it identifies the code of the manufacturer (e.g., Coca-Cola company).

- ***Object Class*** : indicates article classification. The class number must be unique for all given domains (e.g., Coke 280ml can).
- ***Serial Number*** : unique for every class and non-repeating for each object class code (e.g., any unique Coke 280ml can).

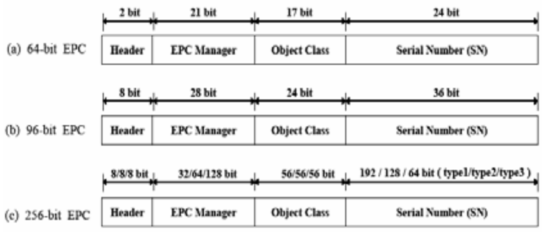

Fig. 1 (a)EPC-64, (b)EPC-96, and (c)EPC-256 bit allocations

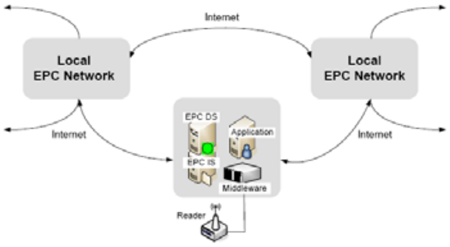

Fig. 2 Global EPC Network Architecture: linking the EPC Network to the Internet [12]

## 2.2 Middleware Service

EPC Middleware manages EPC data received from the reader, provides alerts, and reads information for communication to the EPCIS (EPC Information Services) or the company's other existing information systems. EPC is developing a software interface standard for services enabling data exchange between an EPC reader or network of readers and information systems. EPC middleware designed to process the stream of tag data coming from one or more readers, and this particular piece of software manages readers.

## 2.3 RFID tag and reader

RFID systems are basically composed of tags and readers. An RFID tag, also known as a transponder, is an RFID device consisting of a microchip and antenna attached to a substrate. The microchip in the tag is used for data storage and logical operations, whereas the coiled antenna is used for communication with the reader. When the RFID reader queries, the RFID tag transmits identification information such as an ID, to the RFID reader by means of a Radio Frequency signal. An RFID reader known as transceiver or interrogator. The reader generally consists of an RF module, control unit, and coupling element to interrogate electronic tags via RF communication. An RFID reader receives identification information from an RFID tag and subsequently delivers this information to the RFID middleware. The RFID reader can read and write data on the RFID tags.

The RFID tag is either an active or a passive tag. *active tag* possesses a battery and actively transmits information to the reader for communication. The *passive tag* must be inductively powered from the RF signal of the reader since RFID tags usually do not possess their own battery power supply. The EPC is stored on this tag. Tags communicate their EPCs to readers using a RF signal.

## 2.4 Information Service

EPCIS (EPC Information Services) enables users to exchange EPC-related data with trading partners through the EPC Network. EPCIS provides EPC Network related data available in PML format to request services. Data available through the EPCIS may include tag data collected from EPC middleware such as date of manufacture, expiry date, and product information.

## 2.5 Discovery Service

A Discovery Services enables users to find information related to a specific ID and to request access to that information. In EPC network, An Object Naming Service (ONS) is one component of Discovery Services[11]. The ONS provides a global lookup service, translating EPCs into one or more Internet Uniform Reference Locators (URLs), where further information regarding the object may be retrieved. In short, the ONS provides yellow page services for the EPC Network, allowing participants to quickly discover the server in the EPC Network containing the information associated with a particular EPC. The ONS works same as Domain Name Service (DNS), the foundation naming protocol for the Internet.

## 2.6 Basic RFID System

RFID systems are composed of three main elements: RFID tag, RFID reader, and back-end database. The forward channel, i.e., the reader to the tag, is assumed to be broadcast with an RF signal that can do long-range monitoring. On the other hand, the backward channel, i.e., the tag to the reader, is relatively much weaker, enabling monitoring only by eavesdroppers within the tag's shorter operating range. In general, it is assumed that eavesdroppers can monitor only the forward channel undetected

[12,13,14]. Figure 3 shows the basic RFID system.

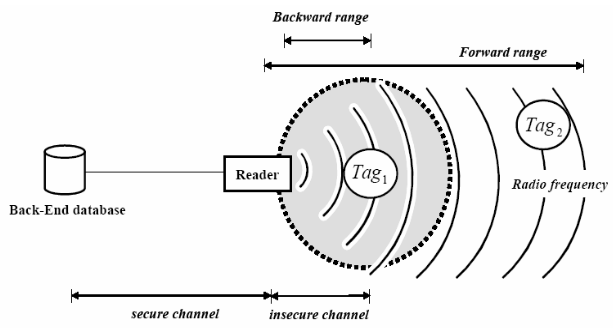

Fig. 3 Basic Passive RFID System [20]

As the data carrier in the RFID system, the *RFID tag or transponder* includes object-identifying data. Tags are generally composed of an IC chip and an antenna. The IC chip in the tag is used for data storage and logical operations, whereas the coiled antenna is used for communication between the reader. The RFID tag may either be *active* or *passive*. The *Active tag* has a battery and actively sends the information to the reader for communication. On the other hand, the *passive tag* must be inductively powered from the RF signal of the reader. Both types of the tag begin to communicate when they are interrogated by the reader. In this paper, the passive type of RFID tag is considered.

- ***RFID reader or transceiver*** is a device that sends an RF signal to the tag, receives the information from the tag, and sends such information to the back-end database. The reader may read and write data to the tag. In general, readers are composed of the RF module, a control unit, and a coupling element to interrogate electronic tags via RF communication.
- ***Back-end database*** is the data-processing system that stores related information (e.g., product information, tracking logs, reader location, etc) with a particular tag.

## 3. Related Work

Until now there are many research results for RFID privacy protection, but we introduce only three of them related to our proposing scheme directly.

### 3.1 Blocker tag

Juels' blocker tag which can be used as a shield for a customer's tags [3,4]. RFID system normally has an anti-collision protocol for reading multiple tags. The blocker tag uses anti-collision protocols reversely for hiding tags. A blocker tag will make a collision whenever any reader tries to scan the tags inside its coverage. Consequently, the blocker tag is one of active jamming devices, and it can be used for illegal purposes such as theft. And it works with the tags inside its physical coverage, but not with the tags logically belonging to the customer.

### 3.2 Using Proxy Device

Another approach is an external device approach, in which a customer uses a proxy device for protecting his or her privacy. There are three representative schemes in this approach; Rieback's RFID guardian project[5], Juels' REP[6], Kim's MARP[7], and Yeo's eMARP[8]. In this approach, an external device serves as a proxy agent for its holder, and it can have a general cryptographic modules and process pretty complicated protocols. And proxy agents seem to be embedded into other mobile devices such as cellular phones and PDA's in the near future. However, there no regulations and standards related to this approach until now, so we need much time to apply these schemes to the current RFID systems.

### 3.3 Backward Channel Protection Scheme

Backward channel protection scheme[9], which is a simple and practical scheme and can be used in the current RFID systems. In this scheme, the reader's action is very important. A reader has to protect the tag's $k$-bit static identifier which is in communication with the reader itself. The reader emits a $k$-bit random number at the same time when the tag emits its static identifier and then this action makes a collision eventually. The reader can resolve this collision because it knows one number of the two collided numbers.

However, passive attackers can't resolve this collision and can't know the tag's static identifier from eavesdropping of backward channel because they can't distinguish the tag's identifier from the reader's random number. Figure 4 show how this protocol works in detail. However, if a reader doesn't provide this protection scheme or an active attacker try to communicate tags directly, the tags emit their static identifier without any protection mechanisms.

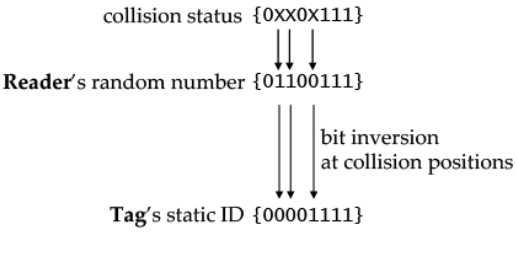
collision status {0XX0X111}
Reader's random number {01100111}
bit inversion
at collision positions
Tag's static ID {00001111}

Fig. 4 Resolving the tag ID from a collision.

## 3. Proposed Protocol

We propose a simple proxy device between reader and tag, and this device is controlled by a customer. A customer uses this proxy device for her privacy protection and for preventing unauthorized tag scanning by attackers. Our proxy device protects all of registered tag in its radio signal coverage. It should be able to connect to public certificate authorities for verifying reader's public key or have an authenticated readers' public key list.

In the case that a customer doesn't have any proxy device or doesn't turn on her proxy device, the current standard RFID protocols are used and any tags of the customer can't be protected from all attacks. In the case that a customer turns on her proxy device, we have to use a new protocol, which can be simply added to the current standard protocols, especially to ISO 18000-6 type C[10].

Figure 5 shows an example of this standard protocol. In this slotted random anti-collision, tags load a random ID into a slot counter, decrement this slot counter based on Interrogator commands, and reply to the Interrogator when their slot counter reaches zero. However, this standard protocol has a big privacy problem that any readers in the radio-frequency range can hear the unique ID of the tag, EPC code.

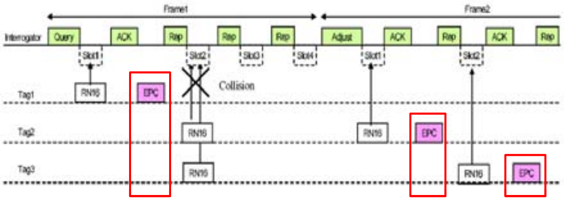

Fig. 5 An operating example of ISO 18000-6 type C.

Our overall protocol can be categorized to four phases; tag registration phase, tag identifying phase, resolving phase for unregistered tags, and resolving phase for registered tags.

### A. *Registration phase*

1. a customer has to register her all tags to her proxy device with their static identifiers.
2. After registration, the proxy device stores all static identifiers of customers' tags into its non-volatile memory. (we assume that the registration phase should be done in secure environment without any threats and we assume that there are some unregistered tags in the proxy device's radio frequency range.)
3. The latter assumption makes our scheme more user-controllable than Juels' blocker tag scheme[3], in which a blocker tag blocks all of the tags in its communication coverage, but not depending on the customer's controlling.

### B. *Tag identifying phase*

1. the reader and the tags follows the standard RFID protocols, but the proxy device do something for protecting registered tags' identifier.
2. After a singulation step, the reader send ACK message to the selected tag for getting the tag's real static identifier.
3. The tag sends its static ID$_i$ to the reader. At the exact same time to the tag's response, the proxy device sends a random number $R_i$ to the reader.
4. The proxy device sends different random numbers $R_i$ to the reader at the same time to each tag's ID$_i$ response. The proxy device stores its all random numbers for all tags which were scanned by the reader and it can resolve the real static identifiers of all tags because it knows all collision bit strings and its own random numbers which were used for making collisions.

In the eavesdropper's view, he can hear only collision bit string and he can know only some bits which are not collided on every tag identification steps. This situation happens to the reader equally. The reader cannot resolve any identifiers of scanned tags, but it stores all collision bit strings, $C_i$, into its memory.

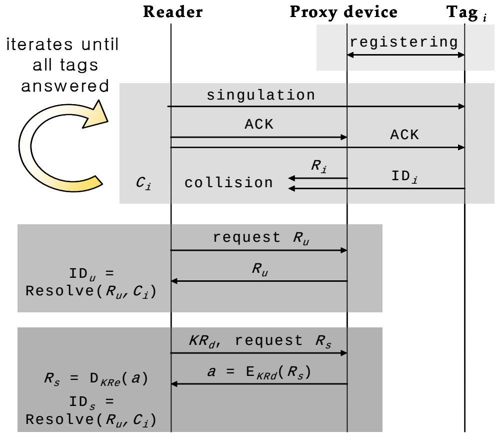

Fig. 6 A modified standard protocol with our proxy device.

### C. *Resolving phase for unregistered tags*

In this phase, the reader requests the proxy device to send the set of random numbers that were used for unregistered tags.

1. The proxy device knows all of its random numbers that were used for making collision and all identifiers of tags that were involved in the prior phase.
2. The proxy also may know which numbers were used for unregistered tags because it has the registered tag list.
3. Then, we can define $R_u$ as the set of random numbers for unregistered tags.
4. The proxy device sends $R_u$ to the reader without authentication because we think that “unregistered” means “unprotected” in the view of customers.
5. The reader can resolve the unregistered tags’ identifiers from comparing $R_u$ and $C_i$.

### D. *Resolving phase for registered tags*

1. The reader requests the proxy device to send $R_s$, the set of random number random numbers that were used for unregistered tags.
2. For completing this phase, the reader has its own public key with a valid registered certificate and it sends the certificate to the proxy device.
3. After receiving the certificate of the reader, the proxy device check whether it is valid or not.
4. A valid certificate means that the reader is authenticated and registered one.

We don’t want to fix the method for checking the validity of the certificate in this scheme. However, it will be a possible method that the proxy device does an on-line transaction with a public certificate authority, CA, for checking the reader’s validity.

If the proxy device should work in off-line environment, it is possible to manage the authenticated readers list and their public key list that may be updated regularly. Anyway,

5. after the proxy device check the validity of the reader and the reader’s public key, the proxy device encrypt $R_s$ with the reader’s public key, $KR_d$ and then send the encrypted message, ***a***, to the reader.
6. The reader can decrypt the message ***a*** with its own private key, $KR_e$. Eventually, the reader can resolve the registered tags’ identifiers from comparing $R_s$ and $C_i$.

Using these mechanisms, we prevent any illegal readers to acquire registered tags’ identifiers and prevent any silent listeners to know the whole identifiers of the tags registered to the proxy device.

## 4. Securities

In this chapter, we analyze the proposed device and its protocol in security point of view.

### A. *Information leakage*

Firstly, we have to address whether this device and its protocol prevent to leak any information about tags. In this scheme, an eavesdropper can acquire some bits of identifier. However, if the tag identifier is long enough, it is very difficult to be guessed by her. Now EPC class 0 tag use 64-bit long code for a static identifier and EPC class 1 generation 2 tag, which is one of 18000-6 standards, uses 96-bit long code. It’s long enough to make difficult to guess tag’s identifier [7]. And an eavesdropper can also hear the message, ***a***, transmitted from the proxy device to the reader. However, only the reader knows its own private key and it can decrypt the message ***a***. There is no information leakage in this case.

### B. *Location Tracking*

Secondly, we need to check whether this scheme prevents illegal location tracking. In this scheme, the same tag emits the same static identifier on every transaction, but the proxy device broadcasts always the different numbers. Therefore an adversary can’t trace the specific tag or its holder, because she can’t distinguish the tag from the others.

### C. *Comparison in Security and on-tag Cost*

We should also consider tag’s hardware cost, which is very important in the view of manufacturers and RFID popularization. Table 1 shows existing privacy protection schemes’ security and their cost on the tag. Most of other schemes need pretty expensive hardware modules for privacy protection, but our proposed scheme need not to be changed on the tag hardware. Therefore our scheme satisfies not only security requirements but also cost requirements.

Table. 1 Comparison in Security and on-tag Cost.

| **Schemes** | **Information leakage** | **Location tracking** | **Changes on the tag** | **Tag cost** |
|---|---|---|---|---|
| Hash locking | strong | weak | small change | cheap |
| Hash-based scheme | strong | weak | hash module | expensive |
| Universal Re-encryption | strong | weak | PKC module | expensive |
| Hash-chain scheme | strong | strong | hash module | expensive |
| MARP | strong | strong | hash module | expensive |
| ***Proposed Scheme*** | strong | strong | nothing | cheap |

## 5. Conclusions

RFID system has become an important technology in the ubiquitous environment. While RFID system brings an idea to fruition, we must consider their security and privacy problems. In particular, although the RFID system enables the logistics management to prevent theft and imitations effectively, it may also allow access to users' private information such as credit information or purchase patterns without their agreement.

Therefore, we proposed a new simple proxy device and a protocol, which can be added to the current existing RFID system such as EPC class 1 generation 2, ISO 18000-6 type C. Our scheme offers a customer to register her tags to her small proxy device for preventing her privacy and location information. This scheme can be adopted for the current RFID standard system with only slight change on the reader, not on the tag. We are sure that it will be cost-effective for RFID tag manufacturer.

## References

[1] R. Anderson, and M. Kuhn, "Low cost attacks on tamper resistant devices", Proceedings of the International Workshop on Security Protocols - IWSP, vol. 1361 of *Lecture Notes in Computer Science*, pp. 125-135, April 1997.

[2] S. Weis, S. Sarma, R. Rivest, and D. Engels, "Security and Privacy Aspects of Low-cost Radio Frequency Identification Systems", Proceedings of the 1st International Conference on Security in Pervasive Computing - SPC 2003, vol. 2802 of *Lecture Notes in Computer Science*, pp. 454-469, March 2003.

[3] A. Juels, R. Rivest, and M. Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy", Proceedings of the Conference on Computer and Communications Security - ACM CCS 2003, pp. 103-111, October 2003.

[4] A. Juels, and J. Brainard, "Soft Blocking: Flexible Blocker Tags on the Cheap", Proceedings of the Workshop on Privacy in the Electronic Society - WPES 2004, pp. 1-7, October 2004.

[5] M. Rieback, B. Crispo, and A. Tanenbuam, "RFID Guardian; A battery-powered mobile device for RFID privacy management", Proceedings of the Australasian Conference on information Security and Privacy – ACISP 2005, vol. 3574 of *Lecture Notes in Computer Science*, pp. 184-194, July 2005.

[6] A. Juels, P. Syverson, and D. Bailey, "High-Power Proxies for Enhancing RFID Privacy and Utility", Workshop on Privacy Enhancing Technologies - PET 2005, May 2005.

[7] Soo-Cheol Kim, Sang-Soo Yeo, Sung Kwon Kim, "MARP: Mobile Agent for RFID Privacy Protection", 7th Smart Card Research and Advanced Application IFIP Conference (CARDIS '06), vol.3928 of *Lecture Notes in Computer Science*, pp.300-312, April 2006.

[8] Sang-Soo Yeo, Soo-Cheol Kim, Sung Kwon Kim, "eMARP: Enhanced Mobile Agent for RFID Privacy Protection and Forgery Detection", The 1st KES Symposium on Agent and Multi-Agent Systems - AMSTA 2007, vol.4496 of *Lecture Notes in Computer Science*, pp.318-327, May 2007.

[9] W. Choi, B.-H. Roh, S.W. Yoo, and Y.C. Oh, "Backward Channel Protection Method for RFID Tag Security in the Randomized Tree Walking Algorithm", *Journal of Korean Institute of Communication Sciences*, vol.30 no.5C, pp.415-421, May 2005.

[10] *ISO/IEC 18000-6:2004/Amd 1:2006* - Extension with Type C and update of Types A and B, June 2006.

[11] D. L. Brock. "The electronic product code (EPC): A naming scheme for objects". Technical Report MIT-AUTOID-WH-002, MIT Auto ID Center, 2001. Available from http://www.autoidcenter.org.

[12] T. Scharfeld. "An Analysis of the Fundamental Constraints on Low Cost Passive Radio-Frequency Identification System Design". MS Thesis, Department of Mechanical Engineering, Massachusetts Institute of Technology, Cambridge, MA 02139, 2001.

[13] D. Engels. "The Reader Collision Problem". Technical Report. MIT-AUTOID-WH-007, MIT Auto ID Center, 2001. Available from http://www.autoidcenter.org.

[14] K. Finkenzeller. "RFID Handbook", John Wiley and Sons. 1999.

[15] D. M. Ewatt and M. Hayes. "Gillette razors get new edge: RFID tags". Information Week, 13 January 2003. Available from http://www.informationweek.com.

[16] S. E. Sarma, S. A. Weis, and D. W. Engels. "Radio-frequency identification systems". Workshop on Cryptographic Hardware and Embedded Systems, CHES02, LNCS 2523, pp. 454-469, Springer-Verlag, 2002.

**Sang-Soo Yeo** received the B.E., M.E., and Ph.D. degrees from Chung- Ang University (Korea) in 1997, 1999, and 2005 respectively. After that, he worked at Dankook University (Lecture Professor) from March, 2006 to February, 2007. He is currently a visiting scholar of Kyushu University, Japan. His main research areas are system security, cryptographic protocols, embedded system securities.

**Jin Kwak** received the B.E., M.E., and Ph.D. degrees from Sungkyunkwan University (Korea) in 2000, 2003, and 2006 respectively. He worked at Kyushu University from April to November, 2006. After that, he joined MIC (Ministry of Information and Communication, Korea) as Deputy Director from November, 2006 to February, 2007. He is currently a professor of Department of Information Security Engineering of Soonchunhyang University in Korea. His main research areas are cryptology, information security, and Ubiquitous computing applications securities.