International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:1, No:10, 2007

# A Study on RFID Privacy Mechanism using Mobile Phone

Haedong Lee, Dooho Choi, Sokjoon Lee, and Howon Kim

***Abstract*—**This paper is about hiding RFID tag identifier (ID) using handheld device like a cellular phone. By modifying the tag ID of objects periodically or manually using cellular phone built-in a RFID reader chip or with a external RFID reader device, we can prevent other people from gathering the information related with objects querying information server (like an EPC IS) with a tag ID or deriving the information from tag ID's code structure or tracking the location of the objects and the owner of the objects. In this paper, we use a cryptographic algorithm for modification and restoring of RFID tag ID, and for one original tag ID, there are several different temporary tag ID, periodically.

***Keywords*—**EPC, RFID, Mobile RFID.

## I. Introduction

RADIO Frequency Identification (RFID) has emerged in order to replace a barcode that has used for the object identification so far. Unlike the barcode system, RFID has many different advantages: it can have data memory in addition to identification data and it can be recognized out-of-sight and from a relatively long distance. These features can enable a more various type of application service in addition to simple identification. For example, it can be inventory management, automation of manufacturing process, shipping management, animal tracking, container recognition, ticketing service.

RFID is the core technology for ubiquitous computing environment implementation, together with USN (ubiquitous sensor network). Currently, there is a new stream, called mobile RFID. Korea plays the main role at mobile RFID research and development. The mobile RFID is the concept and framework that provide end users with a new various services with cellular phone built-in RFID tag chip and/or reader chip, over telecommunication network.

RFID system for manufacturing, supply chain management, shipping management aims at the automation and the efficiency of the business process. At the above application, a security is not a main issue. But mobile RFID is a B2C service for end user. So it may produce various privacy problems into individual person. Privacy issues withhold the prompt and wide spread of RFID service.

This paper is about hiding RFID tag identifier using hand-held device like a cellular phone or personal digital assistance. By modifying the tag ID of objects periodically or manually using cellular phone built-in a RFID reader chip or with a external RFID reader module, we can prevent other people from selecting the information related with objects querying information server with a tag ID or deriving the information from tag ID's code structure or finding the location of the objects and the owner of the objects.

EPCTM Class-1 Generation-2 UHF (860-960 MHz) standard has recently ratified by EPCglobal which is the nonprofit organization charged with promoting the adoption of Electronic Product Code (EPC) technology. This defines the physical and logical requirements for a passive-backscatter, Interrogator-talks-first (ITF), radio-frequency identification (RFID) system operating in the 860 MHz – 960 MHz frequency range. The system comprises Interrogators, also known as Readers, and Tags, also known as Labels. An Interrogator interacts with a Tag by modulating an RF signal in the 860 MHz – 960 MHz frequency range. The Tag receives both information and operating energy from this RF signal. Tags are passive, meaning that they receive all of their operating energy from the Interrogator's RF waveform [1, 2].

We present an overview of the Mobile RFID in Korea, and shopping server at Mobile RFID environment in section II. In section III, we propose Privacy suggestion using mobile phone at and we conclude in section IV.

## II. Mobile RFID

This paper is focused on the individual privacy issues that could occur when he/she buys a RFID tag built-in goods and then keeps the goods in the daily life. We provide the description of the network architecture for mobile RFID service and present on/off shopping process using mobile RFID system. And then we provide privacy protection procedure including protection of location tracking and unauthorized selection of information.

Mobile RFID is the concept and framework that provide end users with a new various services with cellular phone built-in RFID tag chip and/or reader chip, over telecommunication network. In this paper, mobile RFID environment means that mobile RFID devices like mobile (cellular) phone and PDA employing cellular network can be used at querying information of the consumer product related a tag. The mobile RFID devices should have mobile RFID readers which are made for them and are, in particular, compliant with EPCTM Class-1 Generation-2 UHF (860-960 MHz) standard [18]. That

Haedong Lee, Dooho Choi Sokjoon Lee and Howon Kim are with the Electronics and Telecommunications Research Institute (ETRI), 161 Gajeong-dong, Yuseong-gu, Daejeon, 305-350, Korea (e-mail: haenamu@etri.re.kr).

is, Class-1 Generation-2 tags mainly for supply chain are also used for consumer products. Thus, any consumer can get information of a product with a tag by sending an EPC of the tag to an EPC information server with her mobile RFID device in this mobile RFID environment.

Fig. 1 shows mobile RFID service network. The RFID reader built-in handheld devices access data network via telecommunication network like CDMA, WCDMA, and GSM. The system consists of RFID tag built-in objects, RFID reader built-in cellular phone, local ODS server, national ODS server, OIS server, application server. ODS server provides the location of application server or information server. Application server or information server provides the contents or information related with RFID tag.

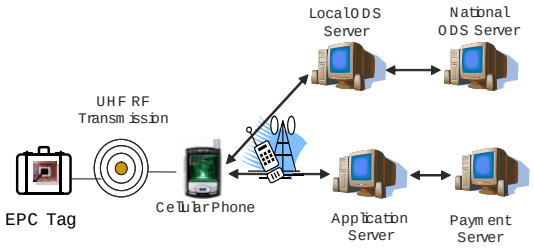


Fig. 1 Mobile RFID Service Network Architecture

The Mobile RFID Service Network consists of four fundamental elements:

1) EPC Tag: The EPC is a globally unique serial number that identifies an item in the supply chain. This allows enquiries to be made about a single instance of an item, wherever it is within the supply chain.
2) Cellular Phone with RFID Reader: cellular phone built-in a RFID reader chip or with a external RFID reader device. Or cellular phone with RFID Tag.
3) Mobile RFID Application Server: Mobile RFID application Server enables users to exchange RFID tag-related data with trading partners through the Mobile RFID Network. And application server provides end users with a new various services like shopping.
4) ODS(Object Directory Service) Server: ODS Server consists of Local ODS and National ODS[3].RFID ODS(Object Directory Service) provides the location of server containing product information related to RFID Tag by using DNS Technology. ODS Server provide the discovery services. The Discovery Services is a suite of services that enables users to find data related to a specific EPC and to request access to that data. The ODS is one component of the Discovery Services.

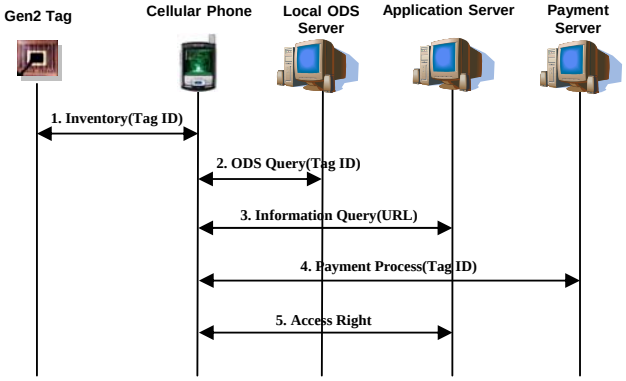


Fig. 2 Shopping Procedure Using Mobile RFID

1. Mobile phone obtains RFID tag ID from RFID tag built-in goods.
2. RFID middleware in the mobile phone send tag ID to Local ODS server. Local ODS server translate tag ID into URL of application server that provide the information and service related tag ID
3. Mobile phone gets the information of goods and the related service.
4. If user wants to purchase the goods, he/she may buy the goods by connecting with the payment system.
5. Finally, mobile phone obtains the tag's kill and/or access password from application server in order to get the access right of RFID tag.

## III. Proposed Privacy Suggestion

In this paper, we assume that RFID tag provide the write lock against the tag code memory bank. In case of using of EPC Class-1 Generation-2(EPC C1G2) standard, passive tag, mobile phone provides write lock and write unlock feature against EPC memory bank. The consumer of the goods with EPC Gen2 tag should download *Access* password and store mobile phone. By connecting POS system or dedicated device, mobile phone can download *Access* password.

Fig. 3 shows the modification process and restoration process of RFID tag ID. The original tag ID ($ID_O$) at Fig. 3 applies the specific code standard. Generally, it is the initial tag ID written by manufacturer or retailer. Mobile phone makes the temporal tag ID ($ID_E$) by using cryptographic algorithm. The original tag ID and secret key ($K$) inside mobile phone is input of cryptographic algorithm. Mobile phone rewrites the EPC memory bank with the output of cryptographic algorithm. In order to make a temporal tag ID continuously into different value, we concatenate original tag ID and random number (*Nonce*) and use it as a input of algorithm. Restoration of the original tag ID can be derived from the output of the decryption algorithm. The input of decryption algorithm is the temporal tag ID and secret key stored at mobile phone.

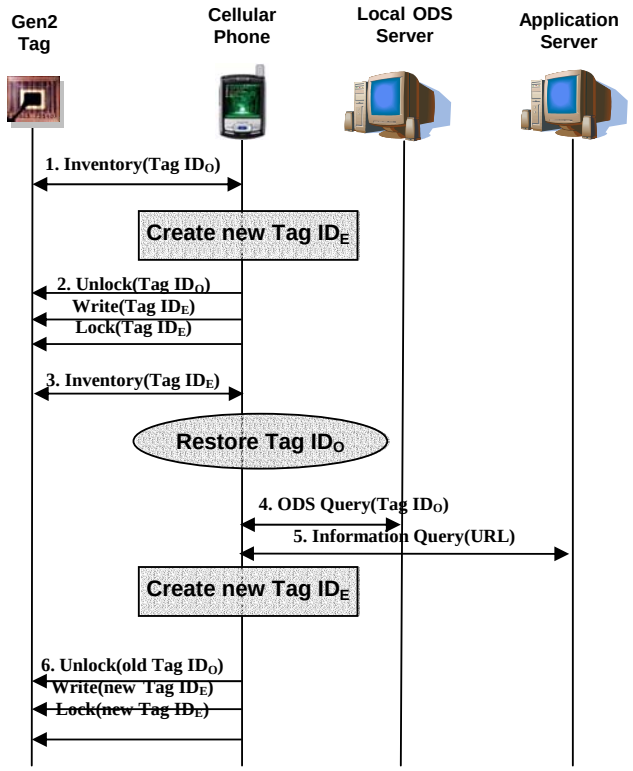


Fig. 3 Procedure of hiding Original Tag ID

As shown at Fig. 3, the procedure of modification applies the following steps.

(1) Mobile phone identifies the original Tag ID ($ID_O$).
(2) Mobile phone makes the temporal tag ID ($ID_E$).
(3) Mobile phone unlocks EPC memory bank using Access password in order to change the tag ID.
(4) Mobile phone rewrites the temporal tag ID ($ID_E$) into EPC memory bank.
(5) Mobile phone locks EPC memory bank using Access password in order not to allow the attacker to write the EPC memory bank on malicious purpose.

Fig. 3 shows how to restore the original tag ID from encrypted tag ID, in order to connect the ODS server and application server located at the backend. The following steps are for it.

(1) Mobile phone identifies the temporal Tag ID ($ID_E$).
(2) Mobile phone restores the original tag ID ($ID_O$).
(3) Mobile phone does ODS Query in order to get the URL of application server.
(4) Mobile phone get the service or contents from application server
(5) Mobile phone makes the new temporal tag ID (new $ID_E$).
(6) Mobile phone unlocks EPC memory bank using Access password in order to change the tag ID.
(7) Mobile phone rewrites the temporal tag ID (new $ID_E$) into EPC memory bank.
(8) Mobile phone locks EPC memory bank using Access password in order not to allow the attacker to write the EPC memory bank on malicious purpose.

The equation below shows how to create the new tag ID. At the start, we obtain the output ($ID_O||Nonce$). Mobile phone makes the temporal tag ID ($ID_E$) by using cryptographic algorithm. The original tag ID and secret key($K$) inside mobile phone is input of cryptographic algorithm.

$$ID_E = E_K ( ID_O||Nonce )$$

$E_K$: *encryption algorithm using secret key(K)*

$||$: *concatenation*

$K$: *secret key stored at mobile phone*

$ID_O$ : *EPC Code(if tag applies EPC standard)*

$ID_E$ : *encrypted EPC Code*

$Nonce$ : *Random number*

The equation below shows how to restore the tag ID from the encrypted tag ID. At the start, we obtain the output ($ID_O||Nonce$). In case that the used tag ID applies EPC Code data standard, tag ID consists of PC and EPC [1], two part. PC is an abbreviation of protocol control bits and we can obtain the length of the (PC + EPC) from PC bits. Finally, we can derive $ID_O$ from $ID_O||Nonce$ and we don't need to remember the Nonce.

$$ID_O||Nonce = D_K ( ID_E )$$

$D_K$ : *algorithm using secret key (K)*

## IV. Conclusion

The method suggested at this paper is intended to solve the following privacy problems: selecting the information of the goods by querying into information server or application server by tag ID, inferring the information of the goods based on the tag code hierarchy and tracking the location of the RFID tag built-in goods or the owner of the goods. From this suggestion, we can find the following effect:

First, because of substituting temporal tag code which doesn't comply with any specific tag code standard for original tag code which complies with a specific code standard, we can prevent an attacker from inferring the information of the goods based on the tag code hierarchy.

Second, the encrypted tag code is not registered at any ODS servers and information servers, application servers, so we can prevent an attacker from gathering the information of the goods related with RFID tag because that anybody can't query to ODS server with encrypted temporal tag code.

Third, because original tag code is always the same, the tracking of tag is possible. Unless encrypted tag code is changed, this tag is trackable. In this paper, by modifying the tag code of objects periodically or manually using cellular

phone built-in a RFID reader chip or with an external RFID reader device, the temporal tag code is always different. So we can prevent tracking the location of the RFID tag built-in goods or the owner of the goods.

## REFERENCES

[1] EPCglobal Web site. www.epcglobalinc.org, 2005.
[2] EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz Version 1.0.9 ttp://www.epcglobalinc.org/stan-dards_technology/EPCglobalClass-1Generation-2UHFRF-IDProtocolV109.pdf
[3] http://www.ods.or.kr/english/overviewOds.jsp
[4] Nokia unveils RFID phone reader. RFID Journal, 17 March 2004. Available at http://www.r-fidjournal.com/article/view/834/1/13.
[5] Ari Juels. Minimalist cryptography for low-cost RFID tags. In C. Blundo and S. Cimato, editors, Security in Communication Networks (SCN 04), pages 149–164. Springer-Verlag, 2004. LNCS no. 3352.
[6] David Molnar and David Wagner. Privacy and Security in Library RFID : Issues, Practices, and Architectures. In B. Pfitzmann and P. McDaniel, editors, Computer and Communica-tions Security, pages 210 – 219. ACM, 2004.
[7] Ari Juels and Ravikanth Pappu. Squealing euros: Privacy protection in RFID enabled bank-notes. In Rebecca N. Wright, editor, Financial Cryptography – FC'03, volume 2742 of Lecture Notes in Computer Science, pages 103–121, Le Gosier, Guadeloupe, French West In-dies, January 2003. IFCA, Springer-Verlag.
[8] P. Golle, M. Jakobsson, A. Juels, and P. Syverson. Universal re-encryption for mixnets. In T.Okamoto, editor, CT-RSA '04. Springer-Verlag, 2004.
[9] RFID Journal Frequently Asked Questions, http://www.rfidjournal.com/faq.
[10] Mobile RFID Forum, http://www.mrf.or.kr.
[11] Stephen A. Weis, Sanjay E. Sarma, Ronald L. Rivest, and Daniel W. Engels. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In Security in Pervasive Computing, volume 2802 of Lecture Notes in Computer Science, pages 201-212, 2004.
[12] The 5-Cent Challenge. RFID Journal, 30 August 2004. Available at http://www.rfidjou-rnal.com/article/articleview/1100/1/2/.
[13] Test Set for RFID-Enabled Phones. RFID Journal, 20 September 2004. Available at http:// www.rfidjourn-al.com/article/articleview/1125/1/20/.
[14] About the EPCglobal Network™. Available at http://www.epcglobalinc.com/about/about _epc_network.html.
[15] IP4 Portable RFID Reader. Available at http://www.intermec.com/eprise/main/Intermec/C-ontent/Products/Products_ShowDetail?Product=RFID2_IP4
[16] Mobile RFID Forum' Launched. IT Korea Journal March~April 2005, page 61. Available at http://www.ica.or.kr/lib/ITKorea_Eng(0503)/052%20industry%20news.pdf
[17] RSA Laboratories. What is the RSA cryptosystem? Available at http://www.rsasecurity.co-m/ rsalabs/node.asp?id=2214.
[18] Mauro Barni and France Bartolini. Data Hiding for Fighting Piracy. In IEEE Signal Processing Magazine, March 2004, page 28 ~ 39.
[19] Stephan J. Engberg, Morten B. Harning, Christian Damsgaard Jensen. Zero-knowledge Device Authentication: Privacy & Security Enhanced RFID preserving Business Value and Consumer Convenience, In Proceeding of PST 2004, page 89~100.