Chapter 20
Implementation of Personalized Wellness Service

Marie Kim, Namje Park and Hyo-Chan Bang

Abstract In this paper, we propose a secure framework for mobile based RFID services using personal policy-based access control for personalized ultra-high frequency (UHF) tags employing the Electronic Product Code (EPC). The framework provides a means for safe use of mobile phone-based RFID services by providing security to personalized wellness service. This new technology aims to provide absolute confidentiality with only basic tags.

Keywords Wellless · Personalized · RFID · Profile

20.1 Introduction

Radio frequency identification (RFID) technology is widely used in supply chain management and inventory control, and is recognized as a strong potential vehicle for ubiquitous computing. However, continued development and global adoption has also raised fears of the potential for exploiting such tags for privacy infringement in 'Big Brother' type scenarios. Thus, information security and privacy protection are as important as standardization of the technology behind the tag, reader, middleware, etc. Conventional authentication algorithms and protocols are not applicable in the greatly resource-limited RFID paradigm, and so new technology should

M. Kim · H.-C. Bang
Electronics and Telecommunications Research Institute (ETRI), 218 Gajeong-Ro,
Yuseong-Gu, Daejeon 305-700, Korea
e-mail: mariekim@etri.re.kr

H.-C. Bang
e-mail: bangs@etri.re.kr

N. Park (✉)
Department of Computer Education, Teachers College, Jeju National University,
61 Iljudong-Ro, Jeju-Si, Jeju 690-781, Korea
e-mail: namjepark@jejunu.ac.kr

J.J. (Jong Hyuk) Park et al. (eds.), *Ubiquitous Computing Application and Wireless Sensor*, Lecture Notes in Electrical Engineering 331,
DOI 10.1007/978-94-017-9618-7_20

be developed in terms of general interconnection among elements and their characteristics of RFID to such technology that meets the RFID circumstances.

The typical architecture of an RFID system, as defined by EPCglobal [1], comprises tags embedded or attached to objects, tag readers that read tag information, and a backend Information Services (IS) server that provides the required information. The tag reader can be designed to be portable or handheld, which allows for several possible applications. While RFID is most commonly used in business-to-business (B2B) commerce for managing supply channels, distribution, and logistics, there is also growing interest in the integration of tag readers with mobile phones, allowing individuals to collect and use tag data, such as in business-to-customer (B2C) marketing. And although current implementations have been limited to movie promotions and museums, where information security is not a major concern, continued development will see more frequent adoption in such fields as retail, medical care, and electrical drafts, where security and privacy are indispensable.

Researchers have developed many techniques to address the various security flaws in RFID systems [6, 8, 9], the simplest being to “kill” tags before they are in the hands of the user [13]. However, because these low-cost tags have numerous applications, the user may want the tag to remain active. As one solution, Rieback et al. proposed the *RFID Guardian* system [12], which relies on a strong proxy device—a mobile phone or PDA—to mediate access by an external reader to tags for auditing of scans and tags, key management, access control, and user authentication. The *RFID Enhancer Proxy* (REP) proposed by Juels et al. requires the use of a similar higher-computing-power proxy device [6] but provides better tag acquisition and ownership transfer. Kim et al.’s *Mobile Agent for RFID Privacy Protection* (MARP) is a further development that aims to provide high-level privacy [8] by employing a public key center that manages keys for the readers, tags, server, and proxy. Kim et al. also recently proposed a scheme suitable for mobile-phone-based reader systems [3], but the method only provides reader-based authentication, which is not sufficient.

Here we propose a secure framework for mobile-phone based RFID services using personal privacy-policy-based access control for personalized ultra-high frequency (UHF) tags employing the Electronic Product Code (EPC). The framework, called M-RPS, has dynamic capabilities that extend upon extent trust-building service mechanisms for RFID systems. This new technology aims to provide absolute confidentiality with only basic tags.

20.2 Strategic Security Framework Architecture

20.2.1 Multilateral Approaches for Improved Privacy

This technology is aimed at RFID application services like authentication of tag, reader, and owner, privacy protection, and non-traceable payment system where stricter security is needed.

- Approach of Platform Level: This technology for information portal service security in offering various mobile RFID applications consists of application portal gateway, information service server, terminal security application, payment server, and privacy protection server and provides a combined environment to build a mobile RFID security application service easily [2, 3].
- Approach of Protocol Level: It assists write and kill passwords provided by EPC (Electronic Product Code) Class1 Gen2 for mobile RFID tag/reader and uses a recording technology preventing tag tracking. Information technology solves security vulnerability in mobile RFID terminals that accept WIPI as middleware in the mobile RFID reader/application part and provides E2E (End-to-End) security solutions from the RFID reader to its applications through WIPI based mobile RFID terminal security/code treatment modules.
- Approach of Privacy Level: This technology is intended to solve the infringement of privacy, or random acquisition of personal information by those with RFID readers from those with RFID attached objects in the mobile RFID circumstance except when taking place in companies or retail shops that try to collect personal information. The main assumptions are privacy in the mobile RFID circumstance when a person holds a tag attached object and both information on his/her personal identity (reference number, name, etc.) and the tag's information of the commodity are connected. Owners have the option to allow access to any personal information on the object's tag by authorized persons like a pharmacist or doctor but limit or completely restrict access to unauthorized persons [4–6].

20.3 Implementation of Personalized Wellness Service

20.3.1 Privacy Policy for Patient Care at a Hospital

We implemented the proposed system for tracking patient care at a hospital. Context-relevant information is important in a ubiquitous computing environment for providing medical care. Different user policies are necessary for patient tags and product tags in EPC global's enterprise application. This ubiquitous sharing system for medical information poses a serious threat to the privacy of personal medical information such location, health, and clinical history. Standards such as Health Level Seven (HL7) do not allow customization and do not include rigorous privacy mechanisms. Therefore, we propose a mechanism that manages privacy policy in a user-centric manner for ubiquitous medical care. It is flexible, secure, and can be integrated with a cryptographic algorithm for mitigating the aforementioned problems.

20.3.2 Design M-RPS Based Customized Service

In a hospital, tags can be used for asset management for location finding. Patient tags are effective in preventing medical accidents, but must be properly designed and constructed to avoid massive collateral damage to user privacy. Hence, we define three-step privacy-aware service architecture for our mobile RFID-based medical application service [14]. The first step is setting the default level of access control over patient information in the default policy. The second step is user-controllable profile-based privacy protection, and the third step is auditable privacy management. Furthermore, we introduce a new RFID-based service model and mobile phone application.

The mobile RFID reader requests for information related to a tag attached to a patient from the backend IS via the middleware system. The mechanism allows individuals to control who can access their personal information. For privacy management, we apply the proposed profile-based privacy management architecture by the addition of a privacy bit to the tag, which is a simple and cost effective mechanism. The privacy bit is the only reference for the privacy service. The medical RFID information server check the privacy guaranteed service or not from the privacy policy. To illustrate how the privacy policy works on the IS, let us consider its use in the application and content information system of the service provider. The privacy level is stored in M-RPS. The RFID code format for the application is defined in the mobile RFID application data format as standard. The default privacy level follows the privacy applied standard of each application service; and if there is no standard, the privacy level is determined based on the results of a privacy impact assessment. The privacy level consists of a 10-tuple of information, where ‘L = L1, L2, …, L10’ as the default privacy policy. It also protected by a secure tag area and privacy server. We also define privacy weights for medical information, as shown in Table 20.1.

Classify the personal medical information by patient’s policy and make personal’s profile. The patient can control his privacy level. Encrypted information can be transferred between the hospital and an emergency transportation service in XML format with security (WS Security) and also can be subject to the standard access control technology for Web services (XACML) (Fig. 20.1).

Table 20.1 Examples of a default privacy weight level

Privacy related people	Privacy weight	Privacy information
Doctor	L4–L9	Medical history treatment information
Nurse	L4–L9	Medical history treatment information
General doctor	L3–L7	Medical treatment
General nurse	L3–L7	Medical treatment
Family	L2–L6	Medical tracking information
Emergency agency	L2–L6	Medical tracking information
Others	L1	All cut off

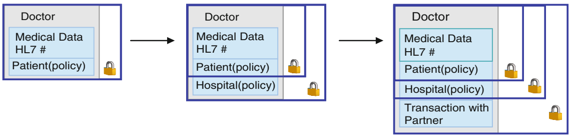


Fig. 20.1 Electronic signature and authentication

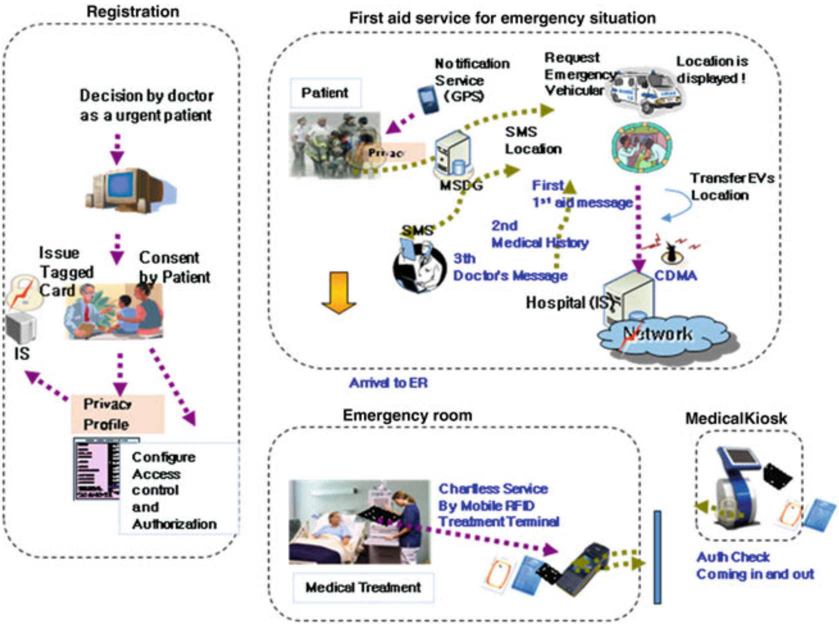


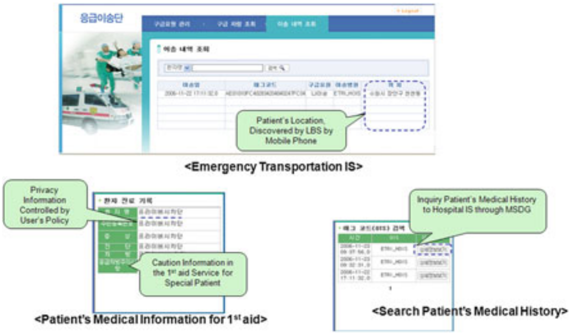
Fig. 20.2 Medical examination with proposed system

In the proposed hospital data management system, RFID-tagged medical card are given to patients on registration. Patients with sensitive conditions, for example, heart disease or cerebral hemorrhage, can use the medical card to rapidly provide medical history that can used for fast application of first aid. Further, biosensors can be incorporated to provide real-time data to the doctor for each specific patient. The RFID patient tags also can be used to verify patient identity to ensure the correct treatment is administered. Thus, the system allows chartless service (Fig. 20.2).

20.3.3 Implementation

The hospital generated an initial set of control data, which included the patient code, medical ID, and related information. The default privacy level was used and

Fig. 20.3 Proposed customized ubiquitous hospital model


응급이송단
Patient's Location, Discovered by LBS by Mobile Phone
<Emergency Transportation IS>
Privacy Information Controlled by User's Policy
Caution Information in the 1st aid Service for Special Patient
<Patient's Medical Information for 1st aid>
Inquiry Patient's Medical History to Hospital IS through MSDG
<Search Patient's Medical History>

the patient was not allowed to control security policy. In order to provide authentication and privacy interface to patient as a agent in medical discovery gateway and hospital's information server system. Essentially, each bit of sensitive data was initially classified by the default privacy weight, which was then modified by the end user's detailed policy. The user-controllable privacy policy in this system evaluation is considered a basic part of RFID privacy management. The compatibility and scalability may be limited, which will hamper system migration, but the mechanism is suitable for policy based privacy control. The proposed privacy management mechanism was implemented in an actual medical emergency room, including a networked medical information RFID kiosk, RFID networked emergency rescue system, and medical examination service, as shown in Fig. 20.3. There is some approach applying the RFID to medicine and hospital. From above, proposed privacy scheme has advantages in custom centric approach aspect for constructing a privacy aware ubiquitous medical system [7, 10, 11, 15].

20.4 Conclusion

RFID technology will evolve to become ubiquitous, allowing automatic detection and delivery of information on the surrounding environment, and interconnecting them through the network. This will require RFID implementation of security measures as the technology is vulnerable to privacy infringement via counterfeiting, falsification, camouflage, tapping, and tracking. Therefore, it is necessary to enact laws and regulations that meet the expectations of consumer protection organizations that are sensitive to individual privacy, and develop and apply secure technologies that can follow such laws and regulations.

Mobile RFID readers are being actively researched and developed throughout the world, and more efforts are underway for the development of related service technologies. Though legal and institutional systems endeavor to protect privacy and encourage data protection, the science and engineering world must also provide suitable technologies. Seemingly, there are and will be no perfect security/privacy protection methods. The technologies proposed in this paper, however, would contribute to the development of secure and reliable RFID systems.

Acknowledgments This paper is extended and improved from accepted paper of UCSWSN 2014, ICHIT2011 conferences. This work was supported by Electronics and Telecommunications Research Institute (ETRI) grant funded by the Korea government. And, this research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2013R1A1A4A01013587).

References

1. Kang T, Lee H, Park D, Bang H, Park N (2013) Creation mechanism for access group based on user privacy policy-based protection. In: MUSIC, pp 125–130
2. Park N (2011) Implementation of terminal middleware platform for mobile RFID computing. IJAHUC 8:205–219
3. Park N (2011) Customized healthcare infrastructure using privacy weight level based on smart device. ICHIT 2:467–474
4. Park N, Lee K, Yoo S, Lee J, Kim Y, Kim H (2011) Secure RFID personal data management using privacy reference profile. In: FGIT, pp 268–276
5. Park N, Kwak J, Kim S, Won D, Kim H (2006) WIPI mobile platform with secure service for mobile RFID network environment. In: Shen HT, Li J, Li M, Ni J, Wang W (eds) APWeb Workshops 2006. LNCS, vol 3842. Springer, Heidelberg, pp 741–748
6. Park N (2010) The implementation of open embedded s/w platform for secure mobile RFID reader. J Korea Inf Commun Soc 35(5):785–793
7. Park N (2011) Secure data access control scheme using type-based re-encryption in cloud environment. In: Katarzyniak R, Chiu T, Hong C et al (eds), vol 381. Springer, Heidelberg, pp 319–327
8. Park N (2010) Security scheme for managing a large quantity of individual information in RFID environment. In: Zhu R, Zhang Y, Liu B et al (eds), vol 106. Springer, Heidelberg, pp 72–79
9. Park N (2012) Mobile RFID/NFC linkage based on UHF/HF dual band's integration in U-sensor network era. In: Park JH, Kim J, Zou D et al (eds), vol 180. Springer, Netherlands, pp 265–271
10. Park N (2014) Design and implementation of mobile VTS middleware for efficient IVEF service. J Korea Inf Commun Soc 39C(6):466–475
11. Park N (2011) Secure UHF/HF dual-band RFID: strategic framework approaches and application solutions. In: Computational collective intelligence. Technologies and applications, lecture notes in computer science, vol 6922. Springer, Heidelberg, pp 488–496
12. Park N (2011) Customized healthcare infrastructure using privacy weight level based on smart device. In: Communications in computer and information science, vol 206. Springer, Heidelberg, pp 467–474
13. Park N (2008) Reliable system framework leveraging globally mobile RFID in ubiquitous era. Ph. D. Thesis. Sungkyunkwan University, South Korea
14. Park N, Kim M (2014) Implementation of load management application system using smart grid privacy policy in energy management service environment. Cluster Computing, vol 17. Springer, New York, pp 653–664
15. Park N (2012) Cell phone based mobile RFID: models, mechanisms and its security. Int J Radio Freq Identif Technol Appl 4(1):67–101