Security Analysis and Implementation Leveraging Globally Networked RFIDs

Namje Park[1,2], Seungjoo Kim[2], Dongho Won[2,*], and Howon Kim[1]

[1] Information Security Research Division, ETRI,
161 Gajeong-dong, Yuseong-gu, Daejeon, 305-350, Korea
{namjepark, khw}@etri.re.kr
[2] Information Security Group, Sungkyunkwan University,
300 Cheoncheon-dong, Jangan-gu, Suwon, Gyeonggi-do, 440-746, Korea
{njpark, skim, dhwon}@security.re.kr
http://www.security.re.kr

Abstract. Mobile RFID (Radio Frequency Identification) is a new application to use mobile phone as RFID reader with a wireless technology and provides new valuable services to user by integrating RFID and ubiquitous sensor network infrastructure with mobile communication and wireless internet. However, there are an increasing number of concerns, and even some resistances, related to consumer tracking and profiling using RFID technology. Therefore, in this paper, we describe the security analysis and implementation leveraging globally networked mobile RFID service which complies with the Korea's mobile RFID forum standard.

1 Introduction

RFID is recognized as the key technology for ubiquitous network which refers to an environment where information can be acquired at anytime and anywhere through network access [10]. RFID technologies consider the environment in which RFID tags are mobile and RFID readers are stationary. On the other hand, in future RFID technologies could consider the environment in which RFID tags are stationary and readers are mobile. RFID based on mobile telecommunications services can be the best example of this kind of usage. RFID based mobile telecommunications services could be defined as services which provide information access through the telecommunication network by reading RFID tags on some objects with a RFID reader in mobile terminals such as cell phones. RFID tags play an important role as a bridge between offline objects and online information. The RFID enabled cell phone was already introduced by Nokia in 2004.

The future RFID tags will be evolved as active tags which have networking capabilities and will be a key component of the ubiquitous network environment rather than current passive RFID tags. In this stage, RFID tags will need network addresses

* Dongho Won is the corresponding author for this paper. The third author of the research was supported by the University IT Research Center Project funded by the Korean Ministry of Information and Communication.

P. Cuenca and L. Orozco-Barbosa (Eds.): PWC 2006, LNCS 4217, pp. 494 – 505, 2006.

for communications. For the ubiquitous network, current RFID related technologies need to be changed to reflect the features of mobile telecommunications services. Also, additional technologies for RFID based mobile telecommunications services should be established to provide harmonized operation of services.

A new security technology is required to provide safe service among mobile RFID tag, terminal, and application to minimize the threat of personal information infringement and leakage as the threat of personal information protection infringement increased due to the mobility of mobile RFID reader, the information leakage due to mobile communication and wireless internet environment is expected, the mobile RFID service can be used illegally and RFID tag information can possibly be counterfeited or falsified. Therefore, in this paper, we describe the security analysis and implementation leveraging globally networked mobile RFID service which complies with the Korea's mobile RFID forum standard. This is new technology to RFID will provide a solution to protecting absolute confidentiality from basic tags to user's privacy information.

2 Networked Mobile RFID Services

Networked RFID means an expanded RFID network and communication scope to communicate with a series of networks, inter-networks and globally distributed application systems. So it makes global communication relationships triggered by RFID, for such applications as B2B, B2C, B2B2C, G2C, etc.

Mobile RFID loads a compact RFID reader in cellular phone, providing diverse services through mobile telecommunications networks when reading RFID tags through a cellular phone. Since the provision of these services was first attempted in Korea, their standardization has been ongoing since 2005. Korea's mobile RFID technology is focusing on the UHF range (860~960MHz), since UHF (Ultrahigh Frequency) range may enable longer reading range and moderate data rates as well as relatively small tag size and cost. Then, as a kind of handheld RFID reader, in the selected service domain the UHF RFID phone device can be used for providing object information directly to end-user using the same UHF RFID tags which have spread widely.

Mobile RFID service is defined as to provide personalized secure services such as searching the products information, purchasing, verifying, and paying for the products while on the move through the wireless internet network by building the RFID reader chip into the mobile terminal [1,2,4]. The service infrastructure required for providing such RFID based mobile service is composed of RFID reader, handset, communication network, network protocol, information protection, application server, RFID code interpretation, and contents development, and the configuration map is as follows.

Mobile RFID service structure is defined to support ISO/IEC 18000-6 A/B/C through the wireless access communication between the tag and the reader, however there is no RFID reader chip supporting all three wireless connection access specifications yet that the communication specification for the mobile phone will be determined by the mobile communication companies. It will be also possible to mount the RF wireless communication function to the Reader Chip using SDR (Software Defined Radio) technology and develop ISO/IEC 18000-6 A/B/C communication protocol in software to choose from protocols when needed.

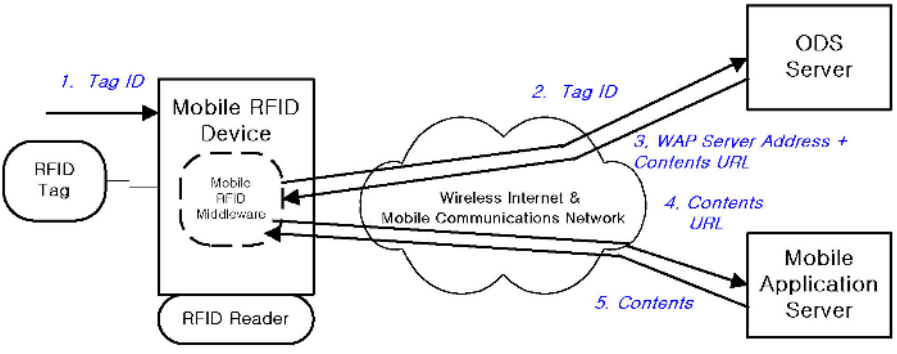

Fig. 1. Basic Communication Model for Mobile RFID Services

Mobile RFID network function is concerned with the communication protocols such as the ODS (Object Directory Service) communication for code interpretation, the message transportation for the transmission and reception of contents between the mobile phone terminal and the application server, contents negotiation that supports mobile RFID service environment and ensures the optimum contents transfer between the mobile phone terminal and the application server, and session management that enables the application to create and manage required status information while transmitting the message and the WIPI (Wireless Internet Platform for Interoperability) extended specification which supports these communication services [2,9,12,14].

The service model, as shown in figure 1, consists of tag, reader, middleware system, and information server. In the point of view of information protection, the serious problem for the RFID service is a threat of privacy [3,5,12]. Here, the damage of privacy is of exposing the information stored in tag and the leakage of information includes all data of the personal possessing the tag, tagged products and location. The privacy protection on RFID system can be considered in two points of view. One is the privacy protection between the tag and the reader, which takes advantage of ID encryption, prevention of location tracking and the countermeasure of tag being forged. The other is of the exposure of what the information server contains along with tagged items [6,7,8]. First of all, we will have a look about the exposure of information caused between tag and reader, and then discuss about the solution proposing on this paper.

3 Mobile RFID-Oriented Security Threats and Requirements

3.1 Some Mobile RFID-Oriented Security Threats

Mobile RFID-oriented security threats are summarized [9,12]. Firstly, RFID tag identifier, ID, can be easily eavesdropped by intercepting broadcasted radio signals or by actively reading RFID tag. Accordingly, it is possible to track RFID-tagged object or monitor the user carrying a specified tag ID using invisible rogue RFID reader. Secondly, RFID tag can contain some important data such as passwords, IDs, user

specific service data for application, etc. Thus, unauthorized tag access can cause denial or misused of service such as a permanent disablement of tag or illegal modification of tag-stored data. Thirdly, Whenever a RFID reader reads a tag ID, its historical reading record like location and time can be collected without agreement of tag user. In especial, if the application of tag is tightly coupled with people, this can cause the violation of privacy due to leakage of the collected historical context data such as the user's preference profile. Finally, Mobile RFID applications need more strict adult verification. Currently teenagers and even elementary school students below 10 are using cell phones which are a ubiquitous information terminal and must be a private device. So they can access adult contents very easily. A strict and elaborate mechanism for adult verification should be provided to protect young people from adult contents. But currently the adult verification is provided within contents at the application layer. That is, the control role is given to contents providers, which means network operators called ISPs cannot control illegal behaviours providing adult contents.

3.2 Security Requirements for Secure Mobile RFID Services

Mobile RFID service structure provides its services by associating the mobile communication network and the RFID application service network based on the RFID tag. The area to consider the security basically is the RFID tag, reader terminal area, mobile communication network area, RFID application service network area, and security issues like the confidentiality/integrity/authentication/permission /non-repudiation shall be considered in each network area. Especially, as the mobile RFID service is the end user service, the issue of privacy protection must inevitably become a serious issue to consider, and as the contents accessibility increases due to the off-line hypertext property of RFID, the authentication for adult service must also become another important issue to consider.

1) Mobile RFID service based on the user's ownership of tagged products needs to guarantee the confidentiality on the tag code information or user data information for personal privacy protection. In this case, mobile RFID application service provider shall provide the confidentiality to the said information or other means to prevent personal privacy infringement.
2) The integrity of the data shall be guaranteed in order to check counterfeiting/falsification of the data transmitted through the communication path in each section of the mobile RFID service network reference structure. However additional code based data integrity other than the least method (for example, CRC) specified in the air interface specification is not required in the communication section between tag and reader terminal considering the limit of the calculation capacity of the tag. However, it is necessary to develop a method to secure the data integrity in the tag for special mobile RFID application service where the personal information is stored in the user data information of the tag and transmitted.
3) The authentication in the mobile RFID can be divided into the device authentication in each network layer and the service user authentication.
   - Device Authentication: Device authentication refers to the authentication of the RFID reader mounted to cellular phone, and mobile RFID service requires the

device authentication as it is based on the inter-working service between heterogenous networks (mobile communication network - RFID application service network).
- User Authentication: User authentication refers to the authentication for mobile RFID service users, and the user authentication is generally required for the reader terminal to access the application server to obtain mobile RFID service contents.

4) The authentication that must be considered in the mobile RFID service structure is as follows.
   - Tag Access Control: Reader terminal can give various commands to the tag, and the tag shall be able to support the access authentication through password especially when executing sensitive commands such as write/delete/lock/kill.
   - Reader Execution Authorization: Refers to the function that verifies whether the user is valid for executing sensitive reader commands such as write/delete/lock/kill at the reader terminal, and it can be possible to develop the reader execution authorization in developing the reader terminal.
   - Authorization for Adult Service: The authorization for adult service is required as the adult content provided by mobile RFID service can be accessed indiscreetly.
   - User Authorization: Must provide the access control for each user or the access object in case of providing different services to each user accessing the application server or differentiating the access level per user.
5) Mobile RFID application service including the processes like bill payment between the reader terminal user and the application server requires the non-repudiation for the data transmitted by the reader terminal user and the application server. In this case, the reader terminal and the application server must be able to execute non-repudiation.
6) Mobile RFID application service that uses the password for halting the tag or authorizing the access to the tag shall be able to safely manage such passwords and safely authorize the key to the reader terminal, and such functions shall be provided by the mobile RFID service infrastructure; for example, the application server or separate key management server.
7) Since mobile RFID service is a B2C service using RFID tag for end users, it inevitably accompanies the issues of personal privacy infringement that it must provide solutions for such issues. The personal privacy issue shall consider both the location privacy relating to the personal identifier role of the RFID tag and the information privacy relating to the identification of personal belongings by browsing the tag interface information through the interpretation of the and the tag code.

4 Key Technology and Solution

4.1 Overview of Secure Networked Mobile RFID Environment

The mobile RFID is a technology for developing a RFID reader embedded in a mobile terminal and providing various application services over wireless networks.

Various security issues - Interdomain security, privacy, authentication, E2E (End-to-End) security, and untraceability etc. - need to be addressed before the widespread use of mobile RFID. Model of mobile RFID service as shown in figure 2 defines additional three entities and two relationships compared to that defined in RFID tag, RFID access network, RFID reader, relation between RFID tag and RFID reader, relation between RFID reader and application server.

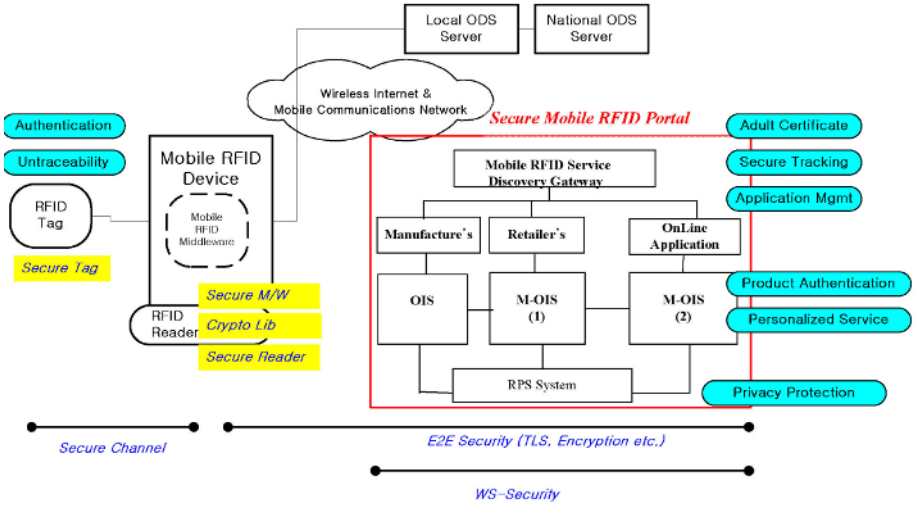

Fig. 2. Conceptual Architecture for Secure RFID over Mobile Networks

Generally, in mobile RFID application such as smart poster, Application Service Provider (ASP) has the ownership of RFID tags. Thus, mobile RFID users have to subscribe to both the ASP for these kinds of RFID services and mobile network operator for mobile communication service. Namely, there exist three potentially distrusted parties: user owned RFID reader, mobile network operator, and ASP. Accordingly, trust relationship among three parties must be established to realize secure mobile RFID service. Especially, when a RFID reader tries to read or change RFID service data stored in tag, the reader needs to get a tag access rights. Additionally, it is important that new tag access rights whenever some readers access a same tag must be different from the already accessed old one.

MRF-Sec 631 strategy represents 6 standard security functions at mobile RFID middleware, 3 major security service mechanisms using 6 security functions, and 1 secure mobile RFID application portal service in order to realize the above 3 security service mechanisms. What is the MRF-Sec 631 strategy? 6-standards security functions are mobile RFID Data encryption API function, mobile RFID secure communication API function, mobile RFID password management API function, EPC C1G2 security command API function, adult certification API function, and privacy protection API function. 3-security service mechanisms are authentication service

mechanism, privacy protection service mechanism, and secure location tracking service mechanism. 1-secure application service is secure mobile RFID application portal service.

4.2 Security Enhanced Mobile RFID Middleware in the Mobile Phone

One of the key problems of the mobile RFID technology is how to quickly use the mobile RFID reader and how to integrate it with the application software installed in the mobile device. In the face of numerous different existing application software, developing a independent mobile RFID middleware layer is a good idea. The mobile RFID middleware layer is in the middle of the RFID reader and the application logic layer. The mobile RFID middleware layer will manage the RFID readers and server for the application logic layer. So the application logic layer based mobile RFID technology can focus on implementing commerce logic.

WIPI is required to come into force on in Korea in case of mobile phone as from 2005 to support interoperability platform for various application software and hardware platform [2]. Therefore we chose WIPI for basic software development platform of mobile phone and the software architecture and the relation between each software functions are shown as figure 3. The software architecture is composed of REX OS, WIPI HAL API, WIPI Runtime Engine, WIPI C API, phone application, Browser parser, and phone GUI. Most functions for mobile RFID technology are designed in the WIPI C API and they are Reader Control, Tag Control, Buffer Control and Filter Control for interfacing with RFID reader and Code Decoder, URN (Uniform Resource Name) Converter, FQDN (Fully Qualified Domain Name) Converter, DNS Resolver and connect Contents Server for communicating with a local ODS server and the contents web server.

In the WIPI specification, the core functions are the functions of handset hardware, native system software, handset adaptation module, run time engine, APIs, and application programs are the areas of the core functional specifications of WIPI. Actually, in the WIPI specifications, only the handset adaptation and APIs are included and the other parts of functions of the wireless Internet platform are considered as the requirements to the handset vendors whether they accept it or not. For example, the run time engine part is required as the mode of download of binary code for its maximum performance.

The core functions of the WIPI are the handset adaptation and APIs which are called 'Handset Adaptation Layer (HAL)' and 'Application Adaptation Layer (AAL)', respectively. The HAL defines an abstract specification layer to support hardware platform independence when porting applications. The AAL defines the specifications for API of the wireless Internet platform. The AAL support the C/C++ and Java programming languages.

Mobile RFID middleware is implemented by extending WIPI platform to provide RF code related information obtained from RF tag through RFID reader attached on mobile phone. Functions of RFID WIPI C API [13] include RFID Reader Control, Buffer Control, Tag Control, Filtering, and Networking for Code decoding, URN conversion, FQDN conversion, DNS resolving and Contents service. WIPI Runtime Engine software for mobile RFID functions is extended to support RFID WIPI C API [11,13] and RFID HAL API. Functions of RFID HAL API include RFID reader

control, Buffer control, Tag control, Filtering, Networking for configuring IP address of Local ODS server. Figure 3 shows middleware functions and software

The RFID device handler provides the definitions for functions of starting the platform and transferring the events from the upper layer of HAL to the RFID H/W Reader. The categories of RFID device handler API cover call, RFID device, network, serial communication, short message service, sound, time, code conversion, file system, input method, font, frame buffer, and virtual key. The AAL provides the definitions for functions of adaptive functions for RFID engine, C/Java API, crypto libraries, and RFID security components.

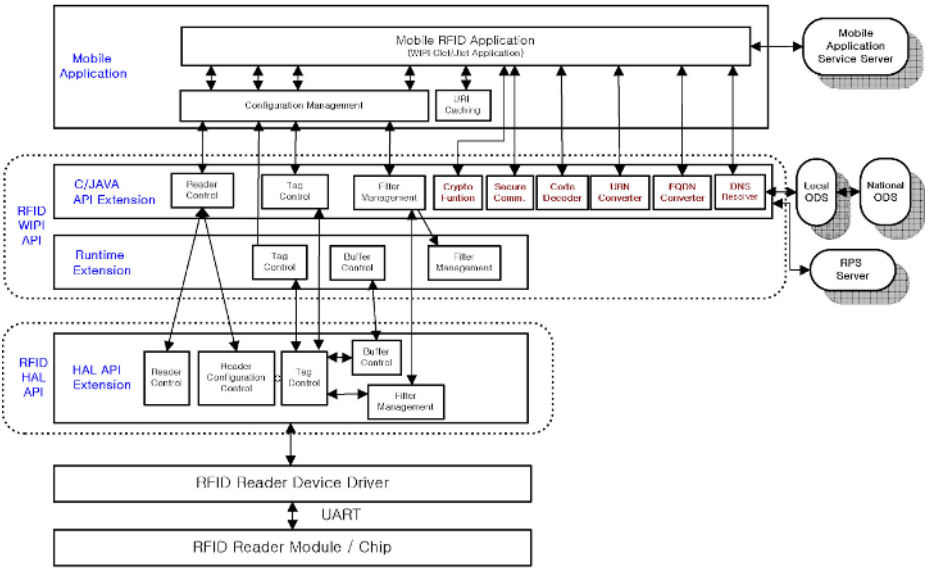

Fig. 3. Security Enhanced Mobile RFID Middleware in the Phone

4.3 Mobile RFID Privacy Protection Service System

Widespread deployment of RFID technology may create new threats to privacy due to the automated tracking capability. Especially, in the mobile RFID environment, privacy problem is more serious since RFID reader is contained in handheld device and many application services are based on Business-to-Costumer model. The RPS (RFID user Privacy management Service) provides mobile RFID users with information privacy protection service for personalized tag under mobile RFID environment [4,8,9]. When a mobile RFID user possesses an RFID tagged product, RPS enables the owner to control his backend information connected with the tag such as product information, distribution information, owner's personal information and so on.

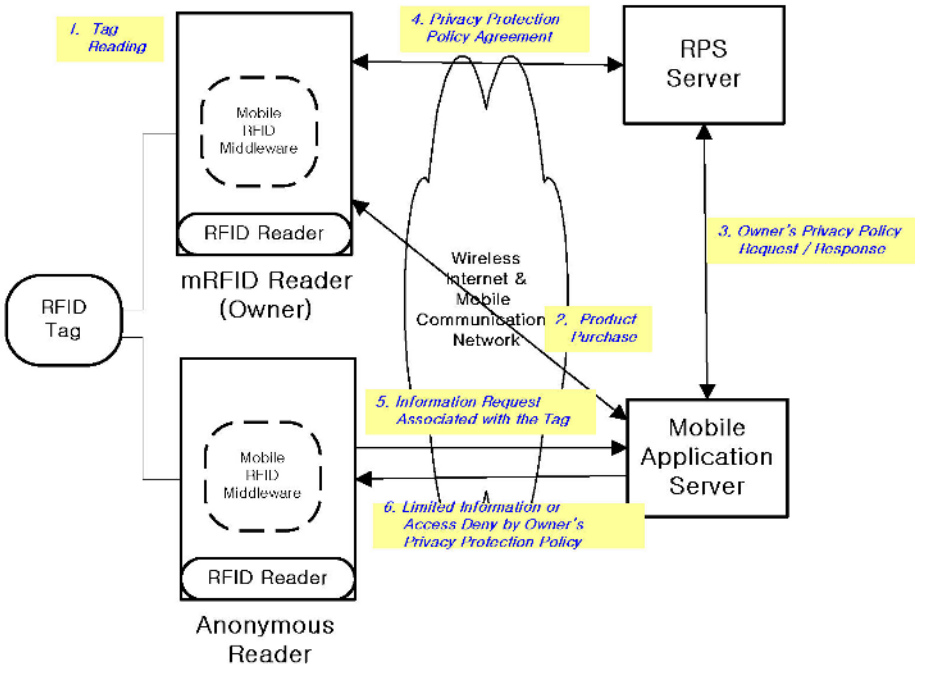

Fig. 4. Service Scenario of RPS Services

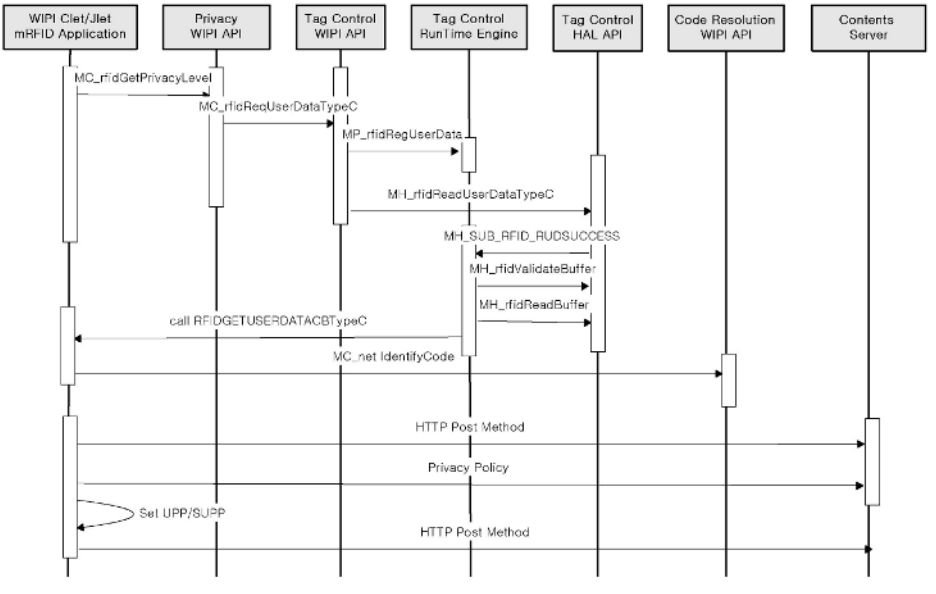

Fig. 5. Procedure of RPS Services

Main features of this service mechanism are owner's privacy protection policy establishment and management, access control for information associated with personalized tag by owner's privacy policy, obligation result notification service, and privacy audit service by audit log management. The brief personal privacy protection process using above functions of RPS is as follows.

Firstly, mobile RFID reader reads the Tag ID and obtains the network addresses of various information such as the product information integrated to the Tag ID through ODS resolver process. Secondly, requests the application server the product information connected to Tag ID. Thirdly, application receives the personal privacy protection policy in relation to the product information through RPS. Finally, the product information is protected appropriately for the privacy protection policy configured by the individual and sent to the reader. The information connected to the Tag ID reflecting personal privacy protection policy through above process is circulated through the network, and it is expected to solve the personal privacy infringement issue through RFID network infrastructure.

4.4 Portal Service System for Secure Mobile RFID Application

Secure mobile RFID application portal is a secure service portal for various mobile RFID application services. The service provider using SMAP (Secure Mobile Application Portal) can easily deploy several mobile RFID applications guaranteed with security and privacy protection.

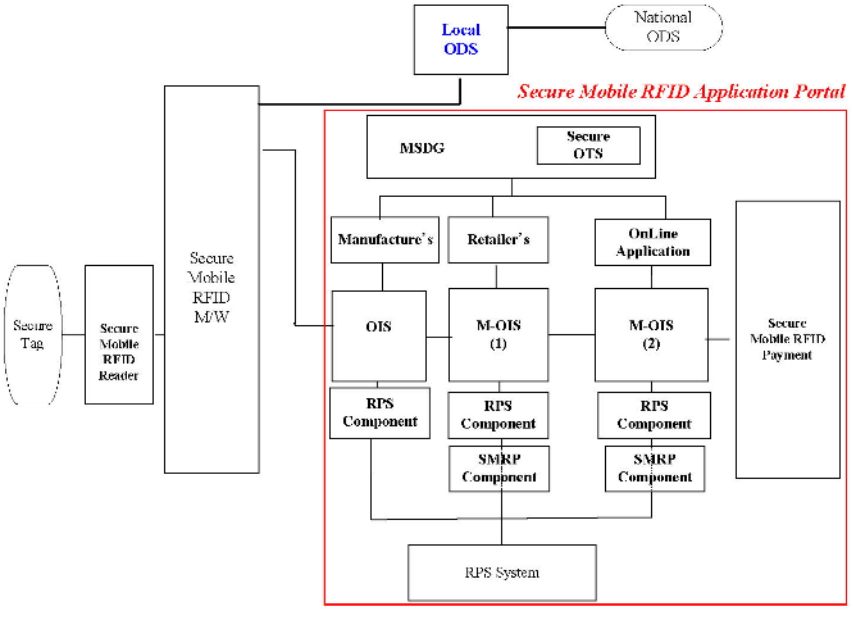

Fig. 6. Architecture of Secure Mobile RFID Application Portal Service

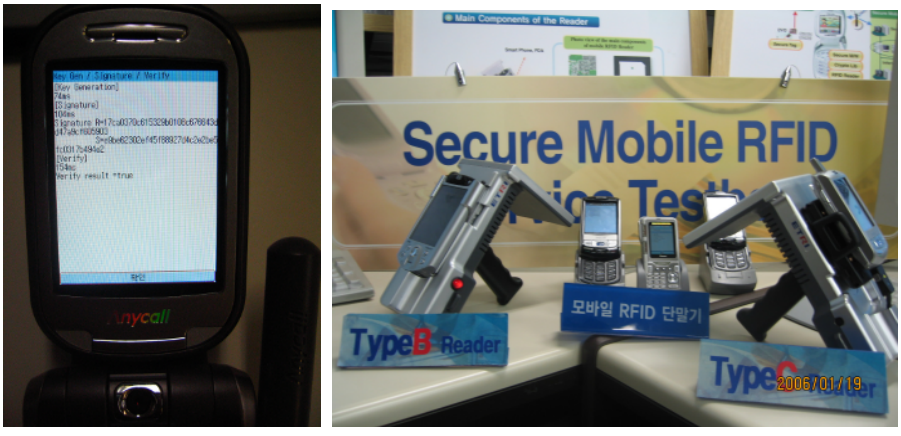

Fig. 7. UHF 900Mhz Mobile RFID Phone Reader

Main features of secure mobile RFID application portal service platform are mobile RFID service discovery, secure object traceability service, application information service, mobile OIS (Object Information Server) generation & management service, mobile RFID privacy protection service, mobile RFID payment service, and mobile RFID security mechanisms - Authentication/Privacy/Untraceability.

5 Conclusion

As mentioned above, mobile RFID is a newly promising application using RFID technology. However, mobility of reader and its service model that is different from RFID service in retail and supply chain will cause some additional security threats.

In this paper, we tried to introduce the concept of mobile RFID and expose some additional security threats caused by it. The frequency band to support the air protocol is allocated at 908.5MHz to 914MHz by TTA (Telecommunication Technology Association) in Korea to comply with ISO 18000-6 for air interface communications at 860MHz to 960MHz. And we describe a way to incorporate its new technology to work with cell phones in particular as an external security reading device (replacing 900MHz) and same time as an added security service to manage all RFID mobile device mediums. With this purpose, the application areas of this service platform are also briefly presented. By doing so, the customized security and privacy protection can be achieved. In this regard, the suggested technique is an effective solution for security and privacy protection in a networked mobile RFID system.

References

1. Tsuji T. Kouno S. Noguchi J. Iguchi M. Misu N. and Kawamura M.: Asset management solution based on RFID. NEC Journal of Advanced Technology. Vol.1, No.3, Summer. (2004) 188-193

2. Jongsuk Chae, Sewon Oh: Information Report on Mobile RFID in Korea. ISO/IEC JTC 1/SC 31/WG 4 N 0922, Information paper, ISO/IEC JTC 1 SC 31 WG4 SG 5 (2005)
3. Seunghun Jin, et. al.: Cluster-based Trust Evaluation Scheme in Ad Hoc Network. ETRI Journal, Vol.27, No.4 (2005) 465-468
4. S. E. Sarma, S. A. Weis, and D.W. Engels: RFID systems, security and privacy implications. Technical Report MIT-AUTOID-WH-014, AutoID Center, MIT (2002)
5. Wonkyu Choi, et. al.: An RFID Tag Using a Planar Inverted-F Antenna Capable of Being Stuck to Metallic Objects. ETRI Journal, Vol.28, No.2 (2006) 216-218
6. Weis, S. et al.: Security and Privacy Aspects of Low-Cost Radio Frequency identification Systems. First International Conference on Security in Pervasive Computing (SPC) 2003
7. M. Ohkubo, K. Suzuki and S. Kinoshita: Cryptographic Approach to "Privacy-Friendly" Tags. RFID Privacy Workshop (2003)
8. Jiwoon Ahn, et. al.: An Analysis of Consumer Preferences among Wireless LAN and Mobile Internet Services. ETRI Journal, Vol.28, No.2 (2006) 205-215
9. Wung Park, Byoungnam Lee: Proposal for participating in the Correspondence Group on RFID in ITU-T. Information Paper. ASTAP Forum (2004)
10. Sangkeun Yoo: Mobile RFID Activities in Korea. The APT Standardization Program (2006)
11. Namje Park, Jin Kwak, Seungjoo Kim, Dongho Won, and Howon Kim: WIPI Mobile Platform with Secure Service for Mobile RFID Network Environment. Lecture Notes in Computer Science, Vol. 3842. Springer-Verlag (2006) 741–748
12. Byungho Chug, et. al.: Proposal for the study on a security framework for mobile RFID applications as a new work item on mobile security. ITU-T, COM17D116E, Geneva (2005)
13. MRF Forum: WIPI C API Standard for Mobile RFID Reader (2005)
14. MRF Forum: WIPI Network APIs for Mobile RFID Services (2005)