CHAPTER 04

SYSTEM FRAMEWORK AND ITS APPLICATION IN MOBILE RFID SERVICE NETWORK

Namje Park*, Rajit Gadh+
Department of Mechanical and Aerospace Engineering, UCLA,
420 Westwood Plaza, Los Angeles, CA 90095,USA
*namjepark@ucla.edu
+ *rgadh@winmec.ucla.edu*

Seungjoo Kim*, Dongho Won+
Information Security Group, Sungkyunkwan University,
300 Cheoncheon-dong, Jangan-gu, Suwon, Gyeonggi-do, 440-746, Korea
*skim@security.re.kr
+ *dhwon@security.re.kr*

Mobile RFID (Radio Frequency Identification) is a newly emerging technology which uses the mobile phone as an RFID reader with a wireless technology and provides new valuable services to the user by integrating RFID and ubiquitous sensor network infrastructure with mobile communication and wireless internet. UHF Mobile RFID technology is based on ISO/IEC 18000-6C can share UHF RFID tags used in logistics/SCM and can avoid redundant investment expected to be integrated with other frequency band RFID. The mobile RFID enables business to provide new services to mobile customers by securing services and transactions from the end-user to a company's existing e-commerce and IT systems. In this paper, we will discuss UHF mobile RFID technology. We begin with a discussion of the details of a mobile RFID system anatomy, followed by a discussion of the components that make up a typical mobile RFID system framework and the underlying sub-systems that make them work.

1. Introduction

RFID (Radio Frequency IDentification) has been recognized as a key technology for ubiquitous networks, which in turn is defined as an environment in which information can be acquired anytime and anywhere through network access service [1,9]. Currently, RFID technologies consider the environment in which RFID tags are mobile and RFID readers are stationary. However, in the future, RFID technologies could consider an environment in which RFID tags are stationary and readers are mobile. RFID based on mobile telecommunications services could 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 certain objects using an 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 introduced by Nokia in 2004 [4,8,9,25].

Furthermore, the RFID tags of the future will evolve as active tags which have networking capabilities, becoming a key component of the ubiquitous network environment rather than the current passive RFID tags. In this stage, RFID tags will need network addresses for communications. For the ubiquitous network, current RFID-related technologies need to be modified to reflect the features of mobile telecommunications services; and additional technologies for RFID-based mobile telecommunications services should be established to provide harmonized operation of such services. In this paper, we will discuss the mobile RFID technology. We begin with a discussion of the details of mobile RFID system anatomy, followed by detailed discussions of the components that make up a typical mobile RFID system framework and the underlying technologies that make them work.

2. Background

In this section, we introduce the overview and basic service models of mobile RFID technology. And, we will discuss the mobile RFID technology's wireless specification, difference of EPC RFID network case.

2.1. *Mobile RFID Technology*

RFID is expected to be the base technology for the ubiquitous network or computing, and is likely to be associated with other technologies such as MEMS (Micro Electro Mechanical Systems), Telematics, and Sensors. Meanwhile, it is widely accepted that Korea is one of the countries that has established a robust mobile telecommunication networks in the world. In particular, about 78% of the population uses mobile phones and more than 95% of those phones have Internet-enabled functions [2, 4, 9]. Currently, Korea has recognized the potential of RFID technology and has tried to converge it with mobile phone. Mobile phones integrated with RFID can be expected to create new markets and provide new services to end-users, and as such will be considered as an exemplary technology fusion. Furthermore, it may evolve its particular functions as an end-user terminal device, or a u-device (Ubiquitous device), in the world of ubiquitous information technology [4, 9, 10, 23, 41].

Actually, the mobile RFID phone may represent two types of mobile phone device; one is the RFID-reader-equipped mobile phone, and the other is the RFID-tag-attached mobile phone. Each type of mobile phone has different application domains: On the one hand, for example, the RFID-tag-attached type can be used as a device for payment, entry control, and identity authentication, and the main feature of this application stems from the fact that RFID readers exist in the fixed position and recognize each phone, giving the user specific services like door opening; on the other hand, the RFID reader equipped mobile phone, to which Korea is currently paying considerable attention, can be utilized to provide end-users with detailed information about the tagged object through accessing the mobile wireless network.

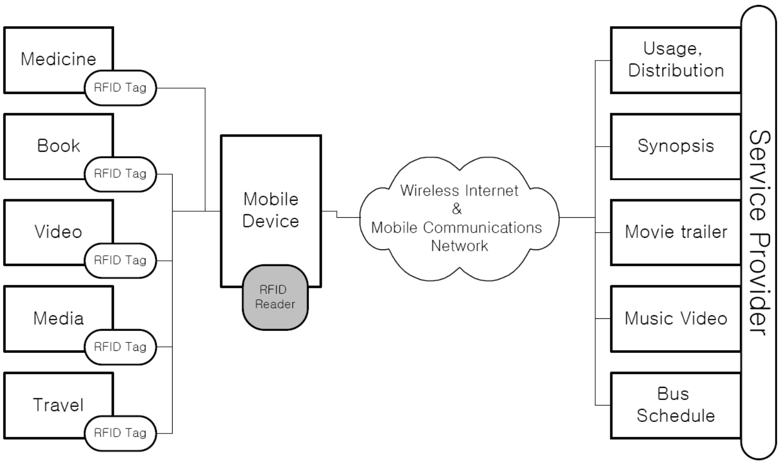


Fig. 1. Example service of mobile RFID for proving Product Information.

The model of the mobile RFID service as shown in figure 2 defines three additional entities and two relationships compared to those defined in the RFID tag, the RFID access network, RFID reader, the relationship between the RFID tag and RFID reader, and the relationship between the RFID reader and the application server.

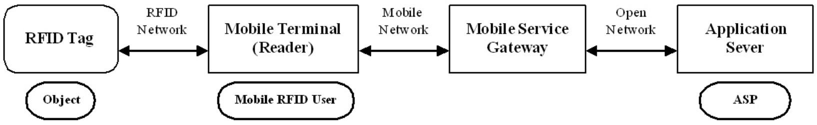


Fig. 2. Model of Mobile RFID Data Communication.

UHF (Ultrahigh Frequency) mobile RFID technology is focusing on the frequency range (860~960MHz), since the UHF range may enable a longer reading range and moderate data rates, as well as a relatively small tag size and lower costs [4, 9, 10]. Then, as a kind of handheld RFID reader, in the selected service domain the UHF RFID phone device can be used to provide object information directly to the end-user using the same UHF RFID tags which have spread widely.

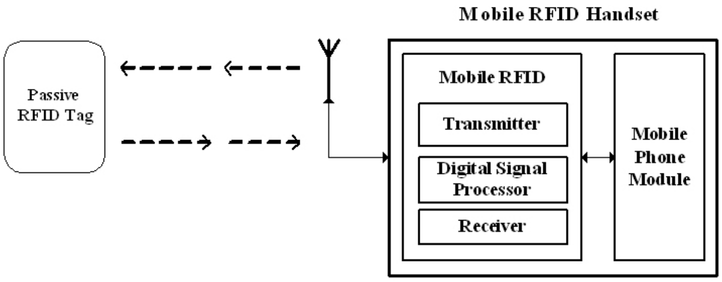


Fig. 3. Mobile RFID Diagram.

2.2. *Mobile RFID's Wireless Specification*

For a mobile terminal with an RFID reader embedded, the configuration of reader chip and adjacent circuitry can be illustrated as shown in figure 4. Inside the reader chip are two components: the digital component, which processes Host/RFID protocols, and the analog component, which processes base band signals and 900MHz RF signals.

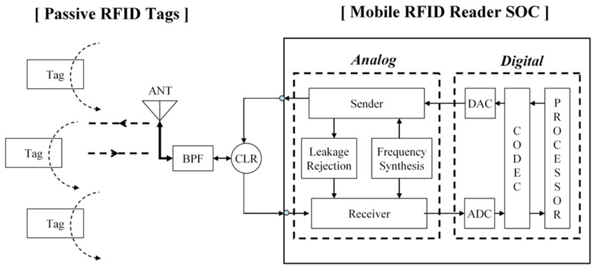


Fig. 4. Mobile RFID's Soc.

To eliminate the analog component from the design, it is necessary to prepare corresponding wireless specifications for it. This chapter prepared the domestic wireless specifications for mobile RFID in Korea, in reference to applicable

RFID frequency, cell radius, channel allocation, and relevant radio regulation acts (ordinances), technical standards, etc.

In general, the minimum power to be delivered to a passive RFID tag is – UHF 10dBm (100uW). On the contrary, since a mobile RFID terminal has good accessibility to tags, it can fully meet the requirements for application in mobile RFID services, if any tag can be recognized within a 1 mile radius. Accordingly, it was estimated that the signal output of a mobile RFID should be at least 20dBm or higher, in overall consideration of link loss = -315dB, tag antenna gain ≤ 2dBi, built-in reader antenna gain ≤ 0dBi, and more. However, a mobile RFID cannot emit as much output as a fixed type reader because it works only with power supplied from a mobile phone battery. Thus, our wireless specifications determined the sender output by allowing for minimum power based on link analysis, limitations of CMOS power amplifier, and the mobile phone’ s battery power.

On the other hand, it is not necessary for mobile RFID to recognize a massive number of tags at once since it is designed primarily for the reader’ s portability. A mobile RFID reader has to only request and send information on several tag recognition codes, so it can make any application service, if necessary, at a data rate of about 40Kbps without difficulty. For example, in Korea, the frequency band allocated for RFID ranges from 908.5MHz to 914MHz. The RFID device supports data rates as high as 640Kbps at this band and can communicate with other terminals only if a wide channel bandwidth is available in the restricted area. It is not appropriate for terminals like mobile RFID that may be used by an uncertain number of multiple users. Therefore, the mobile RFID was based on 200 KHz channel bandwidth at data rate of about 40Kbps.

2.3. *Difference of Features*

2.3.1. *Difference of EPC RFID*

B2B (Business to Business) RFID applications use a similar network configuration to the EPC network as depicted in figure 5. Network configurations for B2C RFID applications are illustrated in figure 6. There are two different properties between such B2B and B2C (Business to Customer) network models. First, the client part, that is, the RFID reader part, is completely different. The B2C model has a single RFID reader without need of controlling multiple readers, but the B2B model has multiple RFID readers and need control of them at a middleware host. The other, final service targets are different. That of the B2C model is human beings and that of the B2B model is business logics, applications and systems. So target contents to be served are different. Such on-line contents as images, audio music, songs, movies, news, games, information, etc., are provided by the B2C model. But on-line contents such as volume of objects, number of packaged boxes, delivery source and destination, expiry date, and so on in different properties, are provided by the B2B model. By these different characteristics, privacy management toward consumers would get important more and existing content servers should be engaged into the B2C RFID network. The following network configuration models consist of various network entities. Addition of functional features count make various networking properties for a network entity and each networking property might make different network architectures.

1) EPC Network Case

A typical RFID network model may refer to the network architecture of EPCglobal as shown in figure 5 where the network entities are RFID tags, readers, ALE host, event management server called EPC-IS, EPC-IS service location server called EPC-DS, and code resolution server called ONS. Business application servers such as ERP, CRM, SCM, etc. are out of scope because they stay at back-end and are associated indirectly with an RFID network. Such a network model is for B2B applications.

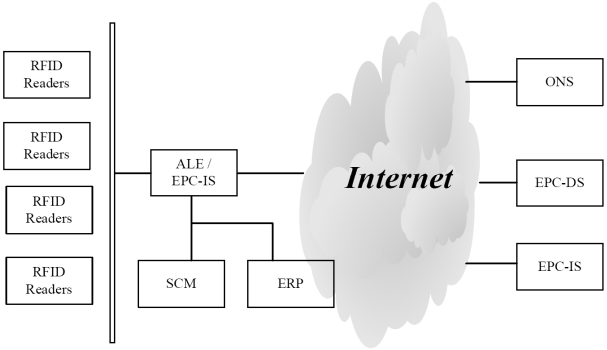


Fig. 5. EPC Network's Configuration.

2) Mobile RFID Case

Changing delivery target of information content to customers, not business applications and business logic entities, enables B2C applications. So delivery targets of B2C contents are consumers, not enterprises. Promising service terminals for B2C network applications are mobile handsets, that is, cell phones in which RFID readers are quipped. Figure 6 illustrates a basic communication model of B2C RFID applications. It consists of two network operations – code resolution and content retrieval. The design philosophy is to consider an RFID reader phone as a client node computer like a desktop PC at which a name resolution is performed first via DNS and a content retrieval is next. Identically, a mobile RFID application client performs a code resolution first via ODS and a content retrieval next. A middleware host is not necessary differently from that of EPCglobal because multiple readers are not engaged in the RFID-reader phone.

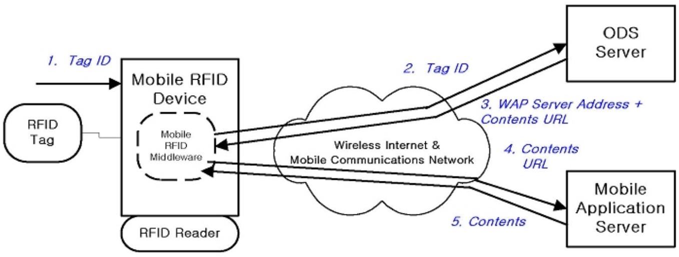


Fig. 6. Basic Communication Model of Mobile RFID.

As the network connectivity expands into consumers, new network entities are installed such as RPS, WAP/Web server, mobile handset, and mobile network infrastructure as shown in figure 6 where OTS is the same to EPC-DS, OIS to EPC-IS, ODS to ONS, additionally RPS and WAP/Web server.

2.3.2. *Classes of Mobile RFID Technology*

For realization of mobile RFID services, it is required that RFID devices such as RFID tag or RFID reader should be installed within mobile phones. The Nokia support RFID technology based on 13.56MHz, MIFARE ®UltraLight, and ISO 14443A. Another mobile phone with RFID functions, the Nokia 3220, is released to public. This Nokia 3220 is based on NFC protocol that uses 13.56MHz complying with ISO/IEC 18092. The Nokia 5140 and 5140i phones as well as 3220 phone with the integrated Xpress-on™ RFID Reader shell is capable of launching services and access phone functions such as dial or send messages by touching an RFID tag. The mobile phone users can automate and initiate tasks, such as browsing service instructions or logging time-stamped data like meter readings.

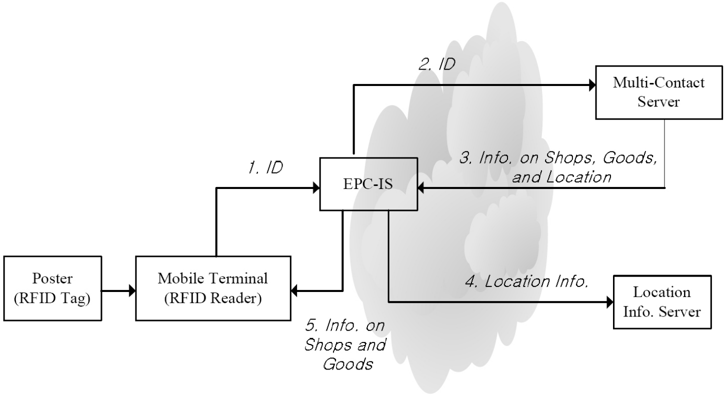
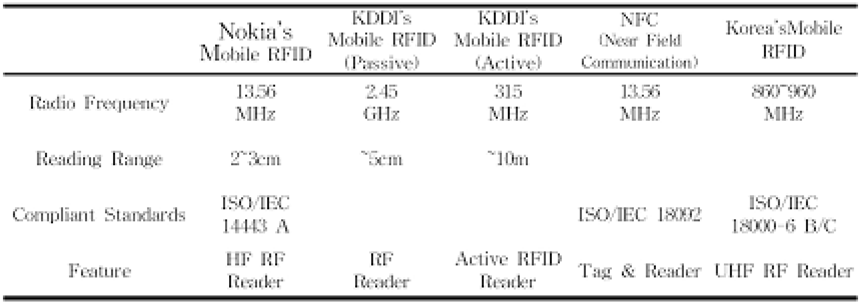

2. ID
Multi-Contact Server
1. ID
EPC-IS
3. Info. on Shops, Goods, and Location
Poster (RFID Tag)
Mobile Terminal (RFID Reader)
4. Location Info.
Location Info. Server
5. Info. on Shops and Goods

Fig. 7. Network Architecture Model of KDDI's Mobile RFID Service.

KDDI in Japan developed slide-in RFID readers that can be easily attached to the back side of a mobile phone. There are two types of RFID reader according to frequency band. One is 2.45 GHz passive type and the other is 315MHz active type. Some pilot tests were scheduled in March 2005. Figure 7 describes KDDI's mobile RFID service architecture. A service broker is located. The multi-contact server seems to provide both code resolution and appropriate contents. Table 1 shows a summary of the possible implementations of mobile RFID.

Table 1. Summary of Mobile RFID Implementations.



	Nokia's Mobile RFID	KDDI's Mobile RFID (Passive)	KDDI's Mobile RFID (Active)	NFC (Near Field Communication)	Korea'sMobile RFID
Radio Frequency	13.56 MHz	2.45 GHz	315 MHz	13.56 MHz	860~960 MHz
Reading Range	2~3cm	~5cm	~10m		
Compliant Standards	ISO/IEC 14443 A			ISO/IEC 18092	ISO/IEC 18000-6 B/C
Feature	HF RF Reader	RF Reader	Active RFID Reader	Tag & Reader	UHF RF Reader

As shown above, UHF-band mobile RFID uses 908.55 ~ 913.95 MHz and complies with ISO/IEC 18000-6 Types B and C [4,12,41]. From the viewpoint of service deployment, the UHF-band is more profitable according to the following observations:

– It has relatively longer range up to 100cm.

Longer range is favorable for most mobile RFID services, ensuring greater convenience.

– *Short range is available up to 2 or 3cm if required* ; in the case of the payment system, short range may be supported by reducing the RF strength by application.

– Avoiding duplicate investment for the RFID tag.

・Most RFID tags in SCM (Supply Chain Management) work in the 900MHz-range, i.e. ISO 18000-6 Types A/B/C and EPCglobal.

・This means that both the SCM and mobile RFID applications can share an RFID tag: thus, a single RFID tag can provide different contents according to its application.

3. UHF-band Mobile RFID Network

3.1. *An Abstract Network Architecture*

Networked RFID comprises an expanded RFID network and communication scope to communicate with a series of networks, inter-networks and globally distributed application systems, engendering global communication relationships triggered by RFID, for such applications as B2B, B2C, B2B2C, G2C (Government to Customer), etc. Mobile RFID loads a compact RFID reader into a cellular phone, thereby providing diverse services through mobile telecommunications networks when reading RFID tags through a cellular phone. Since the provision of these services (ex, mobile RFID using compact UHF RFID chip in cellular phone) was first attempted in Korea in 2005, their standardization has been ongoing. Korea's mobile RFID technology is focusing on the UHF range [4,8,9]. Thus, as a kind of handheld RFID reader, in the selected service domain the UHF RFID phone device can be used to provide object information directly to the end-user using the same UHF RFID tags which have been distributed widely.

The mobile RFID service has been defined as the provision, through the wireless Internet network, of personalized secure services – such as searching for product information, purchasing, verifying, and paying for products – while on the move, by building the RFID reader chip into the mobile terminal [3,11]. The service infrastructure required for providing such an RFID-based mobile service is composed of an RFID reader, handset, communication network, network protocol, information protection, application server, RFID code interpretation, and contents development; the configuration map is as follows.

Figure 8 shows the interface structure for the mobile RFID service's communication infrastructure and the types of relevant standards. RFID wireless access communication takes place between the RFID tag and a cellular phone, CDMA (Code Division Multiple Access) mobile communication takes place between a cellular phone and BTS (Base Transceiver Station)/ANTS (Access Network Transceiver Subsystem), and wire communication takes place between BTS/ANTS and a networked RFID application server.

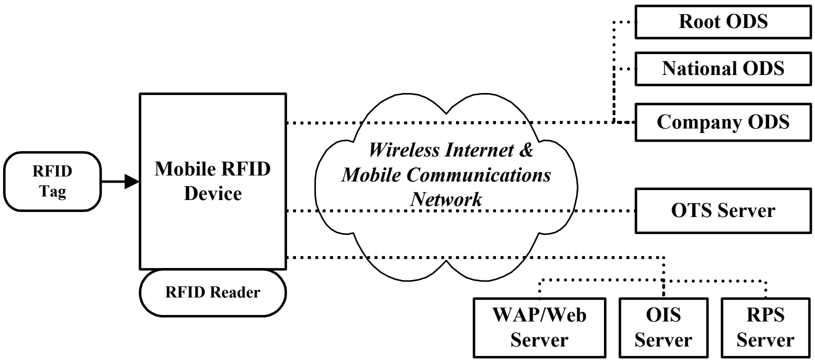


Fig. 8. Conceptual Network Model for Mobile RFID Service.

Figure 8 represents the entities of the mobile RFID service network architecture. The ODS (Object Directory Service) is an information system that provides data needed to obtain an information resource over a network for a specific code expressed in numbers (or mobile RFID's Code). ODS is the same role as EPCglobal’s ONS. The ODS server plays the role of a DNS (Directory Name System) server which informs the mobile RFID phone of the contents/service server’s location, as explained above [9,10,24]. The ODS server may be organized in a hierarchical structure similar to that of a DNS server. The OTS (Object Traceability Service) server keeps a record of the tag readings in the RFID readers throughout the lifecycle of the objects. Its main purpose is to track objects in the SCM. The OIS (Object Information Service) records the reading of the RFID tag event in the OTS server and may provide additional detailed information on an object – such as manufacturing time, manufacturer’s name, expiration time, etc. The RPS (RFID Privacy Management Service) controls access to the information on the object in accordance with the privacy profile put together by the owner of the object. The WAP (Wireless Application Protocol) and Web servers are contents servers that provide wireless Internet contents such as news, games, music, videos, stock trading, lotteries, images, and so forth.

The mobile RFID service structure is defined to support ISO/IEC 18000-6 A/B/C through wireless access communication between the tag and the reader; however, as yet there is no RFID reader chip capable of supporting all three wireless connection access specifications so that the communication specification for the mobile phone will be determined by the mobile communication companies [4,24,26]. It will also be possible to mount the RF wireless communication function on the Reader Chip using SDR (Software Defined Radio) technology and develop an ISO/IEC 18000-6 A/B/C communication protocol in software to choose from the protocols when needed.

The mobile RFID middleware is composed by extending the WIPI (Wireless Internet Platform for Interoperability) software platform to provide RF code-related information obtained from an RF tag through an RFID reader installed in the mobile phone. The networked terminal's function is concerned with the recognition distance to the RFID reader chip built into the cellular phone, transmission power, frequency, interface, technological standard, PIN (Personal Identification Number) specification, UART (Universal Asynchronous Receiver & Transmitter) communication interface, WIPI API (Application Program Interface) extended specification to control the reader chip. RFID reader chip middleware functions are provided to the application program in the form of mobile platform's API. Here, the mobile RFID device driver is the device driver software provided by the reader chip manufacturer.

The mobile RFID network function is concerned with communication protocols such as the ODS 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 the mobile RFID service environment and ensures optimum contents transfer between the mobile phone terminal and the application server, and session management that enables the application to create and manage the required status information while transmitting the message and the WIPI extended specification which supports these communication services [3,8,18,10].

A cellular phone requires a common control interface between the various RFID readers and the application or the middleware; to that end, EPCglobal Inc. and ISO are defining the functions that an RFID reader should commonly support, as well as various common command and standardizing message types. The mobile RFID functions will be extended continuously into standard cellular phone RFID readers, and the RFID supported WIPI extension model using WIPI – the wireless internet standard platform – will define the API required in using the reader suitable for the mobile environment as the API extension of WIPI, while maintaining compatibility among the various devices.

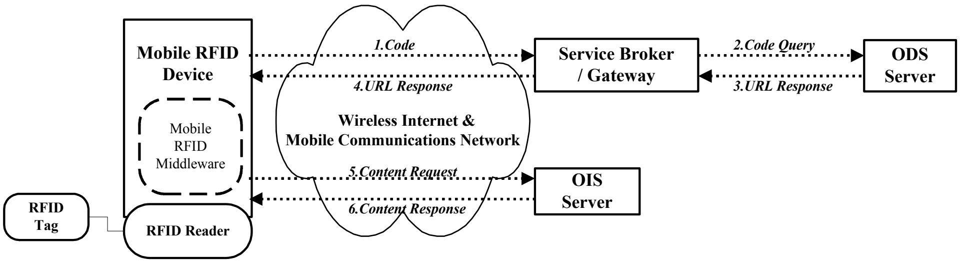


Fig. 9. Block Basic Communication Scenario for Mobile RFID Service.

The basic communication scenario for mobile RFID service is as follows:
First, a mobile RFID phone reads the RFID tags on an object and fetches the code stored in it [8,9,12]. Second, a mobile RFID phone should execute the code resolution with which the mobile RFID phone obtains the location of the remote server that provides information on the product or an adequate mobile service. The code resolution protocol is identical with the DNS protocol. The ODS server in figure 9 as a DNS server and is similar to EPCglobal's ONS (Object Name Service) server. The mobile RFID phone directs queries on the location of the server with a code to the ODS server, then the ODS server replies by giving the location of the server. Finally, the mobile RFID phone requests contents or a service from the designated server whose location has been acquired from the ODS server.

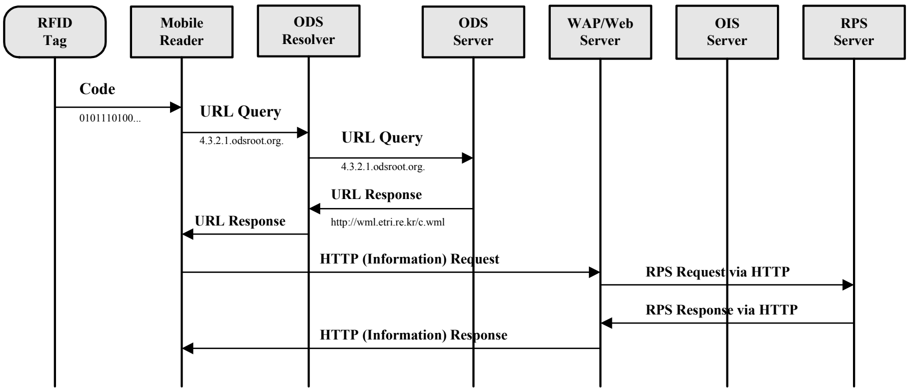


Fig. 10. Detailed Mobile RFID's Code Resolution Process.

Figure 10 illustrates the detailed code resolution process. The code store in the RFID tag is formed of a bit string such as ‘01001101110…’ and this bit string should be translated into a meaningful form such as EPC, mCode (Mobile RFID Code), uCode, ISO Code, or something else [9,23,41,29]. Given that ‘1.2.3.4’ is obtained from a bit string translation and that ‘1.2.3.4’ should be converted into a URN (Uniform Resource Name) form as ‘urn:mcode:cb:1.2.3.4’ , the remaining code resolution process is the same as the DNS reverse lookup process. The mobile RFID reader requests contents retrieval after code resolution. The RFID application in the mobile RFID phone requests contents from the WAP or web server returned by the code resolution.

3.2. *Data Communication Structure*

The mobile RFID service provides requested services by using mCode, micro-mCode, and mini-mCode, defined in this standard, as well as services using attached RFID tag based on EPC code, usually applied in distribution and logistics, and ISO/IEC 15459. This chapter describes code structures like mCode, micro-mCode, and mini-mCode for mobile RFID service and defines RFID tag data structure, where by such codes can be compatible with different code systems. Such code structure helps identify and locate on-line contents and services with unique code structures suitable for mobile RFID service.

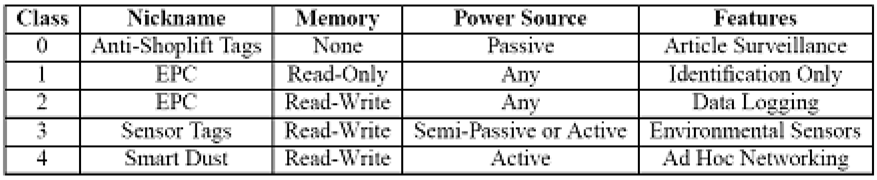
4. Mobile RFID System Components

The mobile RFID service systems are basically composed of RFID tag, mobile RFID reader, ODS system, and OIS system. In this chapter, we explained four key components of mobile RFID service system and forward/backward channel.

4.1. *Passive UHF RFID Tag and Reader*

An RFID tag consist of a microchip and a coupling element - an antenna. Most tags are only activated when they are within the interrogation zone of the interrogator; outside they 'sleep'. Chip tags can be both read-only (programmed during manufacture) or, at higher complexity and cost, read-write, or both. Chip tags contain memory. The size of the tag depends on the size of the antenna, which increases with range of tag and decreases with frequency. Depending on the application and technology used, some interrogators not only read, but also remotely write to, the tags. For the majority of low cost tags (tags without batteries), the power to activate the tag microchip is supplied by the reader through the tag antenna when the tag is in the interrogation zone of the reader, as is the timing pulse - these are known as passive tags. It is also convenient to classify tags by their functionality. The MIT Auto-ID center has defined five classes based on functionality [5, 9].

Table 2. RFID Tag Functionality Classes.



Class	Nickname	Memory	Power Source	Features
0	Anti-Shoplift Tags	None	Passive	Article Surveillance
1	EPC	Read-Only	Any	Identification Only
2	EPC	Read-Write	Any	Data Logging
3	Sensor Tags	Read-Write	Semi-Passive or Active	Environmental Sensors
4	Smart Dust	Read-Write	Active	Ad Hoc Networking

Tag readers interrogate tags for their data through an RF interface. To provide additional functionality, readers may contain internal storage, processing power or connections to back-end databases. Computations, such as cryptographic calculations, may be carried out by the reader on behalf of a tag. The channel from reader-to-tag may be referred to as the forward channel. Similarly, the tag-to-reader channel may be referred to as the backward channel.

In practice, readers might be handheld devices or incorporated into a fixed location. One application of a fixed reader is a 'smart shelf'. Smart shelves could detect when items are added or removed, and would play a key role in a real-time inventory control system. Fundamentally, readers are quite simple devices and could be incorporated into mobile devices like cellular phones or PDAs. A stand-alone, hand-held reader with a wireless connection to a back-end database may cost around US $100-200. If RFID tags become ubiquitous in consumer items, tag reading may become a desirable feature on consumer electronics [37].

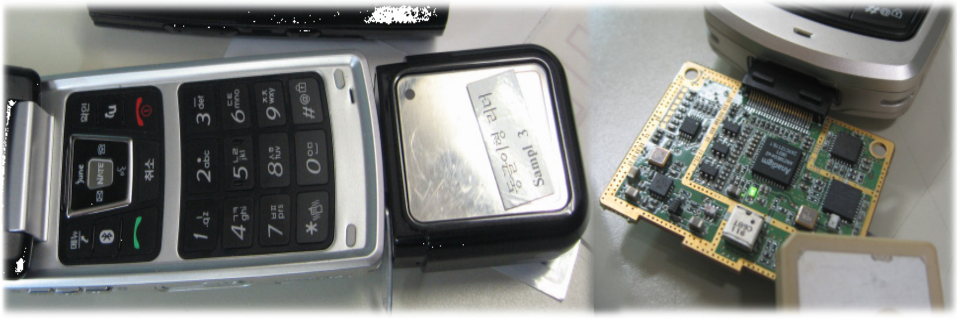


Fig. 11. The mobile RFID Reader.

4.2. Mobile Terminal Platform

WIPI is required to come into force on in Korea in case of mobile phone as from April, 2005 to support interoperability platform for various application software and hardware. Therefore we chose WIPI platform for basic software development platform of mobile phone and the software architecture and the relationship between the various software functions are shown as figure 12. The software architecture is composed of REX OS, WIPI HAL API, WIPI runtime engine, WIPI C API, phone application, quasi-XML 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 CS (Contents Server) for communicating with a local ODS server and the application contents web server [35].

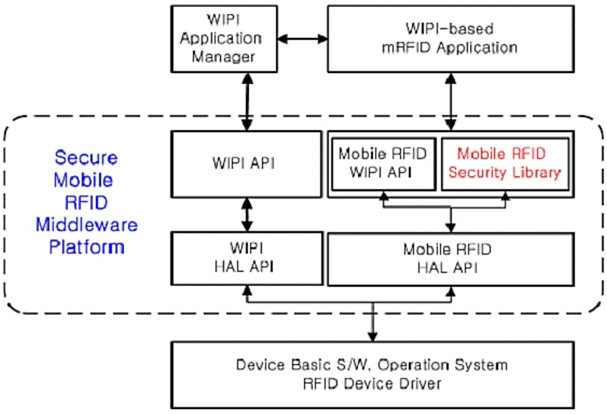

WIPI Application Manager
WIPI-based mRFID Application
Secure Mobile RFID Middleware Platform
WIPI API
Mobile RFID WIPI API
Mobile RFID Security Library
WIPI HAL API
Mobile RFID HAL API
Device Basic S/W, Operation System RFID Device Driver

Fig. 12. Software Architecture in the Mobile Phone.

The mobile RFID middleware is composed 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 [5] 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 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 12 shows middleware functions and software architectures overall. WIPI platform has been set to minimize the side effect that may occur due to the use of various platforms.

4.3. *Back-end Service System*

Local ODS server is a DNS server using UDP port 53 and contents server is a Web server using TCP port 80 for HTTP. In case of failure the code resolution by the RFID reader in the mobile phone, the mobile RFID reader send the unknown code to the local ODS to obtain the location of contents server. Local ODS function architecture as shown in figure 13 consists of the MDM (Multicode Decoding Module), URN/FQDN converter and DNS resolver. Operator has to insert contents server's URL information in zone file in the local ODS server to offer the contents server's location [35].

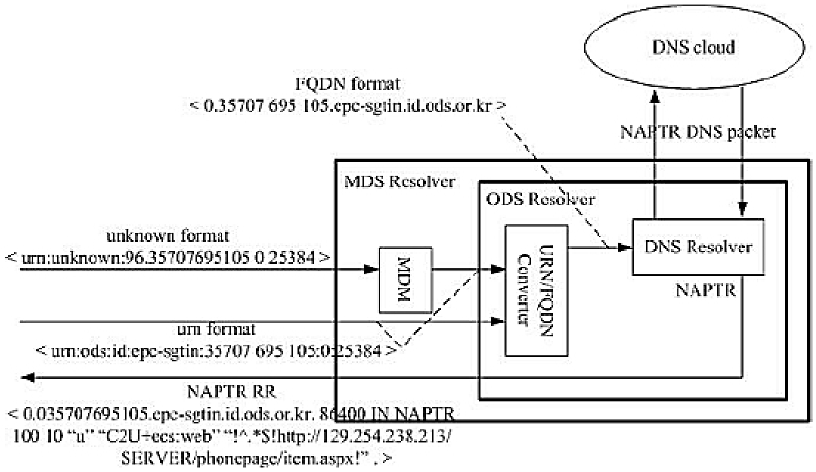

DNS cloud
FQDN format
< 0.35707 695 105.epc-sgtin.id.ods.or.kr >
NAPTR DNS packet
MDS Resolver
ODS Resolver
unknown format
< urn:unknown:96.35707695105 0 25384 >
MDM
URN/FQDN Converter
DNS Resolver
NAPTR
urn format
< urn:ods:id:epc-sgtin:35707 695 105:0 25384 >
NAPTR RR
< 0.035707695105.epc-sgtin.id.ods.or.kr. 86400 IN NAPTR
100 10 "u" "C2U+ecs:web" "!^.*$!http://129.254.238.213/
SERVER/phonepage/item.aspx!" . >

Fig. 13. Local ODS Server System Functions.

The contents server supports B2C services and offers service environments to delivery various contents information to clients. The contents server is able to offer application services including delivery authentication service and tracking service. Tracking and authentication services occur after clients complete their purchases.

1) ODS Resolver Function

In the mobile RFID service environment, the ODS server carries out 'Code Resolution' to look for URI information regarding an RFID code. According to the ODS communication protocol, the ODS resolver gains the URI of the information resources relating to the code and then sends it to the mobile RFID application. User's communication fees depend on what information system contains this ODS resolver. That is, the ODS resolver may be installed within the mobile phone or in the local ODS server of the telecom company. It is highly recommended that the mobile RFID service chooses the latter.

The mobile RFID service has the least ODS resolver function within a mobile phone, the Stub ODS resolver, which sends a query on a code to the ODS server of the telecom company from the mobile phone application. The ODS server plays the role of functions as the ODS resolver, performing Code Resolution with the Root ODS first and other ODS servers according to the ODS hierarchy. The ODS resolver of the telecom company transmits the final URI information to the Stub ODS resolver within the mobile phone and in turn the information is delivered to the application. Through this mechanism, the mobile RFID application within a mobile phone calls for Code Resolution through a one-time ODS query and receives are response message wherein communication traffic occurs much less than when the ODS resolver of the phone carries out the function itself the function.

2) Selecting ODS Resolver

The address of the 'ODS Resolver' or 'Local ODS Server' should be inserted within a mobile phone like setting the DNS server address. The port number of TCP and UDP uses '53,' the same as that of DNS. The basic network information stored in a mobile phone includes the DNS server address that the user may change. Likewise, the ODS server address should be initially put into a mobile phone according to its telecom company by the manufacturer, and the user should be allowed to change it. The purpose of this activity is to comply with the requirements for the open network and service.

3) ODS NAPTR Record

Once the RFID code system is decided, it would have great influence on the overall service infrastructure. If it is a unique code system, objects might need several tags. For example, unlike a beer bottle that is not proper to manage and trace one by one in terms of logistics and distribution, a refrigerator may become an object for individual management and tracing. Since a refrigerator may become a target not only for management and tracing in logistics and distribution but for the mobile RFID service, it would need tags for both services.

If the mobile RFID service adopts the EPC code system, because information resources for the mobile handset-based RFID service differ from those for PDA, desk-top PC, and business systems for logistics & distribution, there may be more than two information resources relating to one EPC code (herein information resources refer to contents). Since a single code may be related to many information resources, a method should be considered to identify the URI information of each information resource and to ask the content server for the wished desired information with a specific URI. To resolve this issue, the ODS NAPTR record regarding a code has to retain information indicating its service kind.

4) Content Negotiation
A mobile phone has a variety of software operation environments. They involve screen size and shape, resolution, color, software implementation platform, browser, input/output interface, and available languages, etc. It may be impossible for users to know these details about their mobile phone, but even if they do, it would be inconvenient to choose their favorite contents for the operation environment through communication with content servers, causing communication charges. Therefore, a mobile phone should ensure at once the optimal contents for the operation environment through prior negotiation with content servers by using efficient negotiation parameters.

5. Selection Criteria for Mobile RFID

The mobile RFID Service Application Requirements Profile (ARP: This describes the requirements for an RFID tag, RFID reader, handset, wireless Internet, network, content server, ODS server, etc. that the mobile RFID service, contents, and technical infrastructure should be equipped with, in from the application service perspective, when the mobile RFID service provides, by means of the B2C method, specific application services such as movie trailers, booking tickets for movies, trains, express buses, and flights, etc. and so on.

The mobile RFID service Common Requirements Profile (CARP: This refers to requirements for RFID tags, readers, handsets, wireless Internet, networks, content servers, ODS servers, service application programs, etc. that the mobile RFID service, contents, and technical infrastructure should be equipped with when the B2C-based mobile RFID service offers common application service as well as specific application services. In other words, this refers to common requirements for all the mobile RFID service applications or common requirements defined in every Application Requirements Profile. The ARP for an application service should contain common application requirements, and if a specific ARP exceeds common requirements, the common requirements should be modified or nullified, otherwise the application service should be announced to be unfeasible.

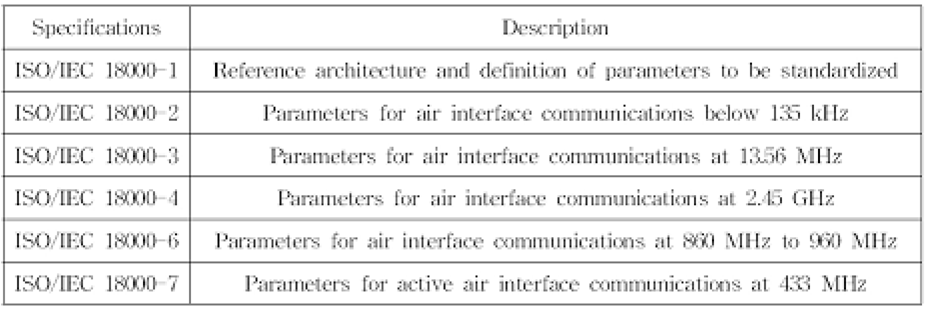
This section includes the common requirements for the mobile RFID services is application service requirements, code system requirements, RFID tag requirements, RFID reader requirements, test requirements, network environment requirements, security requirements.

5.1 *Mobile RFID Service Range*

1) Frequency Conditions

The mobile RFID service standard supports only 900MHz UHF communication based on the ISO/IEC 18000-6. That is, mobile RFID reader chips and tags are communication devices working in the 900MHz frequency range. According to the ISO/IEC 18000 standard, radio frequencies for RFID applications are as follows:

Table 3. ISO/IEC 18000-x wireless access standard.



Specifications	Description
ISO/IEC 18000-1	Reference architecture and definition of parameters to be standardized
ISO/IEC 18000-2	Parameters for air interface communications below 135 kHz
ISO/IEC 18000-3	Parameters for air interface communications at 13.56 MHz
ISO/IEC 18000-4	Parameters for air interface communications at 2.45 GHz
ISO/IEC 18000-6	Parameters for air interface communications at 860 MHz to 960 MHz
ISO/IEC 18000-7	Parameters for active air interface communications at 433 MHz

2) Network Conditions

The mobile RFID service operates based on the TCP/IP and online communication conditions and does not rely on wireless communication network technologies like CDMA2000 1x, 1x EV-DO, 1x EV-DV, WLAN, WCDMA, and WiBro. This implies that once the wireless or mobile communication technologies support TCP/IP, the Mobile RFID service would be accessible under any wireless network.

3) On-line Communication

Portable mobile RFID readers are not always able to handle online communication. The infrastructure components and data flows of the mobile RFID services depend on the circumstances. After reading an RFID tag, the mobile RFID reader can carry out a batch work later over a network. Otherwise, the RFID reader can process the tag data immediately through a network connection. The mobile RFID service provides an environment wherein tag data can be processed at once through wireless Internet because an RFID reader module is installed within a portable handset.

4) Application Software Platform Conditions
The mobile RFID service based on the TCP/IP communication environment uses a reader chip working in the 900MHz built-in RFID reader chip is operated by the WIPI-based platform. The mobile RFID service would be also be available when a WLAN-based handset with a 900 MHz built-in RFID reader and the WIPI application platform is backed by the TCP/IP network communication. In other words, because a PDA handset supported by TCP/IP can run WIPI application programs with its 900MHz reader chip and WIPI platform, the mobile RFID services would be accessible under the WIBRO mobile Internet communication environment.

5.2. ***Application Service Requirements***

Application service requirements do not necessarily rely on mobile RFID technologies in order to be supported by the mobile RFID service infrastructure. Some of them may need technical solutions, but they can also be acquired through the procedure of software system design when a content server creates the content. For such cases, this standard does not suggest the solutions for the application service requirements, regarding but regards them as achieved. Yet this standard specifies the requirements for mobile RFID tags, readers, mobile phones, wireless Internet, networks, content servers, and services that need mobile RFID technologies and specifications.

1) Active Application Software Operation
When the user selects the relevant application software for a tag code, it should be downloaded for installation and implementation. If it is already downloaded, the user is able to use it. Different application software may be used depending on the tag code.

2) Identical Code Multiple Application Service Model
A specific tag code should not be limited to one single application service. One product can access multiple service models because each service model may choose an individual tag, or one single tag may involve all related services. Therefore, there can be multiple services (WAP site, application software) for a

certain tag code, and the user should be able to carry out the wished desired service from among them.

Take a music record, a record company would want to promote the record, a record shop sell the record, and customers listen to it first before buying. They could diverge from a single service, but they might need each different service model because they are distinct service providers. For example, the record shop might want its own bargain sale event for a certain record. Therefore, a tag code should be able to access multiple services.

3) Variable Multiple Application Service Model

The service relating to a tag code should provide the user with a different content depending on the circumstances. For example, during an event period, the tag code will connect to the service like the event introduction and prize contest. After the event, it may announce prize winners or provide other services. For another example, the user would be provided with product information before buying, but manuals, repair service, and maintenance information after buying. The service also varies depending on the places. A refrigerator at a shop is for promotion or selling, one at a showroom for promotion, and one at home for use. A record is for promotion or selling at a shop, but one at home is an item for maintenance.

4) Independent 'Read' and 'Implementation'

Reading the tag code by the reader and using application services for the code should be separate operations. That is, the user may carry out services immediately after reading the tag code or later using the saved tag code.

5) Manual Code Input

In case that the reader fails to read the tag due to any tag/reader problems or unidentifiable reasons, application programs should support a user interface to input the tag code by hand. This is an optional requirement.

6) Save Application Program Status

The start or stop of a mobile RFID application service is not necessarily performed only when the mobile phone is on. Even though the mobile phone happens to turn off in the middle of the application service, the service should remain as it is. As for the mobile shopping, the user should be able to see the previous purchasing information when the mobile phone is turned on again, and the payment should be completed after buying all wanted items even as the phone happens to turn on and off several times during the procedure in the middle. This is an optional requirement because not all application service models need this requirement.

5.3. *Code System Requirements*

This section is not for requirements description. Instead, it aims to define the conditions and characteristics of code systems to help decide one for the mobile RFID service. There are three kinds of codes for RFID application services. They are EPC made by EPCglobal, ISO/IEC 15963 and 15459 by ISO/IEC, and ucode by the Ubiquitous ID center. It has to be decided whether to choose one from among them or whether to create one's own unique code structure.

For the mobile RFID application service model, a real object serves as a medium between information resources on a network and a user. The RFID code performs functions of the medium, and the physical tag can be compared to a bowl containing a code. Information resources to be conveyed to humans need to be expressed in a way that human senses can recognize through a mobile phone that has a limited data input/output environment.

Considering such a service characteristic, since the mobile RFID service is supposed to target a people sharing the same culture and language and is actually the an exclusive wireless Internet contents environment, a nation can choose its own unique code structure for the service without adopting the code system promoted by international organizations or market leading institutions. Therefore, selecting a unique code structure could be a feasible alternative.

5.4. *Tag, Reader Requirements*

1) Save Single Code

The mobile RFID service must save only a single code as UII in a tag. In case there are more than two codes, the first read code is accepted with and the rest are ignored.

2) User Data Field

There are various kinds of tags including a tag that contains just code information or that can store application data in its user data field for the application service. The mobile RFID service should be able to employ two such two kinds, and the latter tag is used as follows:

The user data field is used by a content service provider or the mobile RFID application within a mobile phone. The former is optional and the latter required.

Therefore, in mobile RFID application programs or WIPI API, the user data field must be available as described in section 4.2.

Since a content provider optionally uses optionally the user data field, it saves data in there when necessary. For the mobile RFID service, the process explained in section 3.1 should be done before code resolution and other procedures. Code resolution can take place after the process of section 2.1, otherwise the service may terminate without code resolution.

3) Mobile RFID Reader Module

When constructing the whole infrastructure for application services, reader's functionality is an important element in defining overall data flows and mutual interface. That is because it depends on the reader's functionality to decide whether a specific task will be performed by the reader or other systems.

For the mobile RFID service infrastructure, only one RFID reader is mounted within a mobile phone, which does not require a host system to manage multiple readers. Some functions of the ALE host system on EPC network are integrated into a mobile phone with application programs, and the mobile RFID phone would become the integrated RFID reader system. The integrated RFID reader system of the mobile RFID service can serve as an assumed service broker between a handset and content servers by diminishing communication traffic and processing information for additional services. Yet the service broker is not considered a common requirements for the mobile RFID service, and it would not affect the requirements for the reader system construction. As for the service broker, its network structure and relevant standards are discussed in separate documents.

6. Enforcing Security in Mobile RFID Environment

The mobile RFID is a technology for developing an RFID reader to be embedded in a mobile terminal and for providing various application services over the wireless networks. Robust mobile RFID security must both protect service network against security threat and shield consumers from privacy intrusions. The keys to robust mobile RFID security are simplicity and a fundamentally secure foundation. This section looks at these security points and recommends an alternative approach to achieving robust mobile RFID security. This section aims at providing secure mobile RFID services, and analyzing secure mobile RFID service models to solve security issues like security among domains, personal privacy profile, authentication, end-to-end security, and track prevention.

There are many ways to interfere with RFID circumstances, issues which are not only approved theoretically but also possible practically. Besides security vulnerabilities in RFID security like passive signal interception attack on RFID tags and readers, reading of RFID tags by unauthorized readers, falsifying tag or reader identity, use of attack tools against RFID tags, neutralization of RFID tags, and elaborate attack on RFID tags with cryptographic hacking methods, there are also similar vulnerabilities and possible infringement of privacy in mobile RFID circumstances. It requires proper security technologies. Furthermore, needed are some information protection service models that ensure security and privacy protection and management for service providers in practical compliance with present RFID specifications and mobile RFID standards even when tags do not use code algorithms. This chapter suggests and analyzes these mobile RFID information protection service models considering situations mentioned above. The provision of secure mobile RFID services needs a combined security framework resolving many security issues like security among domains, personal privacy profile, authentication, end-to-end security, and track prevention.

7. Conclusions

As mentioned above, mobile RFID is an emergent and promising application that uses RFID technology. However, the mobility of reader and its service model – which differs from the RFID service in the retail and supply chain – will give rise to additional security threats.

To address these issues, while both are important tools, neither killing nor recoding is the final answer in RFID privacy. The killing alone is not enough, and new mechanisms are needed for building privacy-preserving RFID architectures. In this chapter, we have tried to introduce the concept of mobile RFID and expose some of the additional security threats caused by it. The frequency band to support the air protocol is allocated from 908.5MHz to 914MHz in Korea in order to comply with ISO 18000-6 for air interface communications at 860MHz to 960MHz. We also describe a way of incorporating the new technology to work with cell phones in particular, both as an external security reading device (replacing 900MHz) and as an added security service to manage all RFID mobile device mediums. With this purpose in mind, the application areas of this service platform are also briefly presented. By doing so, 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 service system.

Acknowledgments

This work was supported by the Korea Research Foundation Grant funded by the Korean Government (KRF-2008-357-D00255). The authors thank the members of the RFID/USN research team at ETRI for formulating many of the concepts discussed in this chapter. The authors also thank to all members of Wireless Internet for Mobile Entertainment Consortium (WINMEC http://winmec.ucla.edu/) and the UCLA RFID Lab (http://winmec. ucla.edu/rfid/), University of California at Los Angeles. Due to the introductory character of this chapter, some of the material that provides detailed information relevant to the topic of the chapter is not included. Readers interested to know more about matter described here are directed to conference papers and more technical information on mobile RFID's security are Namje Park's web site: http://www.security.re.kr/~njpark.

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, 188 (2004).
2. Klaus Finkenzeller, RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification, *Wiley (2003).*
3. Sullivan L., Middleware enables RFID tests, *Information week*, no.991, (2004).
4. Jongsuk Chae, and Sewon Oh, Information Report on Mobile RFID in Korea. ISO/IEC JTC1/SC 31/WG4 N0922, *Information paper*, ISO/IEC JTC1 SC31 WG4 SG 5, (2005).
5. 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).
6. Weis, S. et al, Security and Privacy Aspects of Low-Cost Radio Frequency identification Systems, *First International Conference on Security in Pervasive Computing,* (2003).
7. M. Ohkubo, K. Suzuki, and S. Kinoshita, Cryptographic Approach to ‘Privacy-Friendly’ Tags, *RFID Privacy Workshop, (2003).*
8. Wung Park, and Byoungnam Lee, Proposal for participating in the Correspondence Group on RFID in ITU-T, *Information Paper,* ASTAP Forum, (2004).
9. Sangkeun Yoo, Mobile RFID Activities in Korea, *Contribution Paper of the APT Standardization Program, (2005).*
10. Yongwoon Kim, and Noboru Koshizuka. Review report of Standardization Issues on Network Aspects of Identification including RFID, *ITU-T, Paper TD315, (2006).*
11. Mitsuo Tsukada, and Atsunobu Narita, Development models of network aspects of identification systems (including RFID) (NID) and proposal on approach for the standardization, ITU-T, *JCA-NID Document 2006-I-014*, (2006).
12. Baehyo Park, Seoklae Lee, and Heugyoul Youm. A proposal for personal identifier management framework on the Internet. ITU-T, *COM17-D165, (2006).*
13. 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, 741 (2006).

14. Namje Park, Seungjoo Kim, Dongho Won, and Howon Kim, Security Analysis and Implementation leveraging Globally Networked Mobile RFIDs, *Lecture Notes in Computer Science*, vol.4217, Springer-Verlag: 494 (2006).
15. Gildas Avoine, and Philippe Oechslin. RFID traceability, A multilayer problem, In Andrew Patrick and Moti Yung, editors, *Financial Cryptography – FC'05*, vol.3570 of *Lecture Notes in Computer Science.* Springer-Verlag, 125 (2005)
16. Y. Yutaka, and K. Nakao, A Study of Privacy information Handling on Sensor Information Network, *Technical report of IEICE*, (2002).
17. ITU-T TSAG RFID CG Deliverable, Review report of Identification based Business Models and Service Scenarios, (2006).
18. 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, Q9/17, *Contribution 116*, Geneva, (2005).
19. Doogo Choi, Howon Kim, and Kyoil Chung, Proposed draft of X.rfidsec-1: privacy protection framework for networked RFID Services. ITU-T, COM17C107E, Q9/17, *Contribution 107*, Geneva, (2007).
20. Jin Kwak, Keunwoo Rhee, Soohyun Oh, Seungjoo Kim, and Dongho Won, RFID System with Fairness within the Framework of Security and Privacy, *Lecture Notes in Computer Science*, vol.3813, Springer-Verlag, 142 (2005).
21. Simson Garfinkel, Ari Juels, and Ravi Pappu, RFID privacy: An overview of problems and proposed solutions, *IEEE Security and Privacy*, 3(3), 34 (2005).
22. MIC (Ministry of Information and Communication) of Korea, RFID Privacy Protection Guideline*. MIC Report Paper,* (2005).
23. Junseob Lee, and Hyoungjun Kim, RFID Code Structure and Tag Data Structure for Mobile RFID Services in Korea, *Proceedings of ICACT,* (2006).
24. Yoshito Sakurai, and HyoungJun Kim, Report for Business Models and Service Scenarios for network aspects of identification (including RFID), ITU-T, *TSAG TD 314,* (2006).
25. Nokia. RFID Phones – Nokia Mobile RFID Kit, http://europe.nokia.com/nokia.
26. TU-T TSAG, A Proposed New Work Item on Object/ID Associations, (2005).
27. Mobile RFID Forum of Korea, WIPI C API Standard for Mobile RFID Reader, *Standard Paper, (2005).*
28. Mobile RFID Forum of Korea, WIPI Network APIs for Mobile RFID Services, *Standard Paper, (2005).*
29. Mobile RFID Forum of Korea, Mobile RFID Code Structure and Tag Data Structure for Mobile RFID Services, *Standard Paper,* http://www.mrf.or.kr, (2005).
30. Mobile RFID Forum of Korea, Access Right Management API Standard for Secure Mobile RFID Reader, MRFS-4-03, *Standard Paper*. http://www.mrf.or.kr, (2005).
31. Mobile RFID Forum of Korea, HAL API Standard for RFID Reader of Mobile Phone. *Standard Paper, (2005).*
32. Mobile RFID Forum of Korea, WIPI API for Mobile RFID Reader Device. *Standard Paper, (2005).*
33. Frank Thornton et. Al. RFID Security. *Andrew Williams*, (2006).
34. Katherine J. Strandburg, and Daniela Stan Raicu, Privacy and Technologies of Identity : A cross-disciplinary conversation. *Springer,* (2005).

35. Myunghee Son, Yongjoon Lee, and Cheolsig Pyo, Design and Implementation of mobile RFID technology in the CDMA networks, *Proceedings of ICACT, (2006).*
36. Hyangjin Lee, and Jeeyeon Kim, Privacy threats and issues in mobile RFID, *Proceedings of the First International Conference on Availability, Reliability and Security*. vol.1, (2006).
37. Stephen A. Weis, Sanjay E. Sarma, Ronald L. Rivest, and Daniel W. Engels, Security and Privacy Aspects of Low-Cost Radio Freguency IdentiÞcation Systems. *Proceeding of First International Conference on Security in Pervasive Computing,* (2003).
38. Byunggil Lee; Howon Kim; Kyoil Chung; The design of dynamic authorization model for user centric service in mobile environment, Vo1.3, pro. of *ICACT 2006,* (2006).
39. Divyan M. Konidala, and Kwangjo Kim, Mobile RFID Security Issues. *Proceeding of Symposium on Cryptography and Information Security*, (2006).
40. Yongwoon Kim, Junseob Lee, Sangkeun Yoo, and Hyoungjun Kim, A Network Reference Model for B2C RFID Applications, *Proceedings of ICACT,* (2006).
41. Simson Garfinkel, and Beth Rosenberg, RFID: Applications, Security, And Privacy. *Addison-Wesley, (2005).*
42. Steven Shepard. RFID : Radio Frequency Identification. *McGraw-Hill,* (2005).
43. Xiaoyong Su, Chi-Cheng Chu, B.S. Prabhu, and Rajit Gadh, On the Identification Device Management and Data Capture via WinRFID Edge-Server, IEEE Systems Journal, 1(2), 95-104, (2007).
44. B.S. Prabhu, Xiaoyong Su, Harish Ramamurthy, Chi-Cheng Chu, and Rajit Gadh, WinRFID – A Middleware for the enablement of Radio Frequency Identification (RFID) based Applications, Invited chapter in Mobile, Wireless and Sensor Networks : Technology, Applications and Future Directions, Rajeev Shorey, Chan Mun Choon, Ooi Wei Tsang, A. Ananda (eds.), John Wiley & Sons, Inc., 331-336, (2006).