Cell phone-based mobile RFID: models, mechanisms and its security

Namje Park

Department of Computer Education,
Teachers College,
Jeju National University,
61 Iljudong-ro, Jeju-si,
Jeju Special Self-Governing Province, Korea
Email: namjepark@jejunu.ac.kr
Email: namjepark@gmail.com

Abstract: Mobile Radio Frequency Identification (RFID) 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. 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 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.

Keywords: RFID; radio frequency identification; mobile RFID; middleware; embedded platform; privacy; network architecture; ubiquitous; mobile; EPC; WIPI; wireless internet platform for interoperability.

Reference to this paper should be made as follows: Park, N. (2012) 'Cell phone-based mobile RFID: models, mechanisms and its security', *Int. J. Radio Frequency Identification Technology and Applications*, Vol. 4, No. 1, pp.67–101.

Biographical notes: Namje Park is currently an Assistant Professor at the Department of Computer Education, Teachers College in Jeju National University, Korea. He received the BSc degree in Information Industry from Dongguk University, Korea, in 2000, and received his MS and PhD degrees in Computer Engineering from Sungkyunkwan University in 2003 and 2008, respectively. He was a Senior Engineer in the Information Security Research Division at the Electronics and Telecommunication Research Institute (ETRI) and he had worked as a post-doc at UCLA and Arizona State University. His current research interests are RFID/sensor network and a variety of cryptographic technologies.

1 Introduction

Radio Frequency Identification (RFID) has been recognised 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 (Tsuji et al.,

2004; Yoo, 2005). 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 RFID 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 (Nokia, 2004; Park and Lee, 2004; Chae and Oh, 2005; Yoo, 2005).

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 harmonised operation of such services. In this paper, we will discuss the mobile RFID technology. We begin with a discussion of the details of a mobile RFID system anatomy, followed by detailed discussion 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 and difference of EPC RFID network case.

2.1 UHF mobile RFID technology

The main philosophy of the networked RFID is that it tries to remove data from the tag and manipulates the data on the network (Sarma et al., 2002). Therefore, it makes the code which tag holds as small as possible. The size of the code, which is defined by EPCglobal, is 96 bits or 128 bits. This small code size makes the cost of RFID tag cheap and resolving operations efficient. All information related to the code (i.e. the tagged object) is stored on the database server on the network, and the RFID application gets the information of the RFID tag by the aids of specially designed naming services such as Object Naming Service (ONS) (Weis et al., 2003; Avoine and Oechslin, 2005).

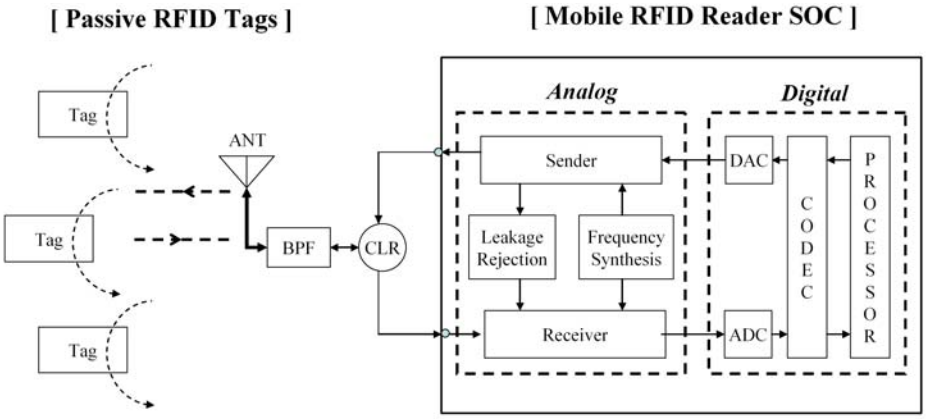
When we briefly review the networked RFID architecture, which was proposed by EPCglobal, it consists of three major components such as: ONS, EPCIS and EPC-DS (EPC Discovery Service). The ONS resolves the RFID code (EPC number) in the networked RFID. Its role is similar to Domain Naming Service (DNS). The EPCIS is a database that contains the information related to the code, i.e. the tagged object. The information can be product model number, price, weight, manufacturer, distributer, etc. The EPC-DS tells the networked RFID about the location of EPCIS where holds the information of the specific RFID code (Weis et al., 2003). EPCglobal proposed this networked RFID for B2B RFID applications such as supply chain management, logistics and manufacturing management. It consists of a number of RFID readers.

The networked RFID technology has been focused on the UHF (860–960 MHz) band, since UHF-banded RFID tag can be read longer and faster than the Low Frequency (LF) and High Frequency (HF) banded RFID tags. The reason is as follows: though the intensity of the magnetic field in HF can be well defined for a specified read zone, it quickly downs as the function of distances from the antenna. In comparison, the electric field used in UHF is relatively faster and enables read distances up to about 10 metres. Additionally, EPCglobal chose the UHF-banded RFID tag because of the possible applications to item-level RFID tagging. However, there is still controversy which frequency-banded RFID tag is better (ITU-T TSAG, 2006; Kim et al., 2006).

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 1. Inside the reader chip are two components: the digital component, which processes host/RFID protocols, and the analogue component, which processes base band signals and 900 MHz RF signals.

Figure 1 Mobile RFID's SOC



To eliminate the analogue component from the design, it is necessary to prepare corresponding wireless specifications for it. This section 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. (Lee et al., 2006).

In general, the minimum power to be delivered to a passive RFID tag is – UHF 10 dBm (100 μW). 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 recognised within a 1 mile radius. Accordingly, it was estimated that the signal output of a mobile RFID should be at least 20 dBm or higher, in overall consideration of link loss = –315 dB, tag antenna gain ≤ 2 dBi, built-in reader antenna gain ≤ 0 dBi, 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 recognise 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 40 kbps without difficulty. For example, in Korea, the frequency band allocated for RFID ranges from 908.5 MHz to 914 MHz. The RFID device supports data rates as high as 640 kbps 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 40 Kbps.

2.2.1 Transmitter

The frequency band of mobile RFID ranges from 908.5 to 914 MHz, and the bandwidth of each channel is 200 kHz. Channel spacing for frequency designation is also 200 kHz, and channel numbers according to frequency allocation are shown in Table 1.

Table 1 Channel no. and channel band according to frequency allocation of mobile RFID

Channel no.	*Channel band*	*Channel centre frequency*	*Channel no.*	*Channel band*	*Channel centre frequency*
	908.50–908.75 MHz	Lowest Guard Band			
1	908.75–908.95 MHz	908.85 MHz	14	911.35–911.55 MHz	911.45 MHz
2	908.95–909.15 MHz	909.05 MHz	15	911.55–911.75 MHz	911.65 MHz
3	909.15–909.35 MHz	909.25 MHz	16	911.75–911.95 MHz	911.85 MHz
4	909.35–909.55 MHz	909.45 MHz	17	911.95–912.15 MHz	912.05 MHz
5	909.55–909.75 MHz	909.65 MHz	18	912.15–912.35 MHz	912.25 MHz
6	909.75–909.95 MHz	909.85 MHz	19	912.35–912.55 MHz	912.45 MHz
7	909.95–910.15 MHz	910.05 MHz	20	912.55–912.75 MHz	912.65 MHz
8	910.15–910.35 MHz	910.25 MHz	21	912.75–912.95 MHz	912.85 MHz
9	910.35–910.55 MHz	910.45 MHz	22	912.95–913.15 MHz	913.05 MHz
10	910.55–910.75 MHz	910.65 MHz	23	913.15–913.35 MHz	913.25 MHz
11	910.75–910.95 MHz	910.85 MHz	24	913.35–913.55 MHz	913.45 MHz
12	910.95–911.15 MHz	911.05 MHz	25	913.55–913.75 MHz	913.65 MHz
13	911.15–911.35 MHz	911.25 MHz		913.75–914.00 MHz	Highest guard band

The tolerance of transmit frequency sent from mobile RFID should be set to less than ±10 ppm in a temperature of –25°C to +40°C and up to ±20 ppm in a temperature of –40°C to +65°C. The modulation method of a mobile RFID should be either DSB-ASK, SSB-ASK or PR-ASK. When a mobile RFID uses one of the designated modulation methods specified above, the occupied frequency bandwidth of each channel must be below 200 KHz. When RF signals transmitted from a mobile RFID occur during power-up or power-down, they create envelope waves depicted in Figure 2. The factor value related to the envelope shape according to time belongs to the norms shown in Table 2.

Figure 2 Envelope wave of transmit signal

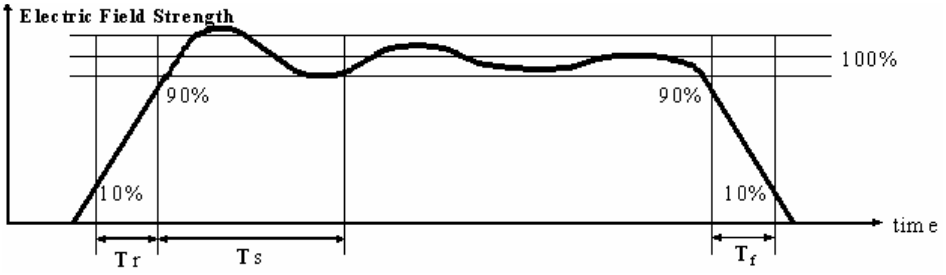


Table 2 Envelope wave parameters of transmit signal

Rising time (T_r)	*Stable time (T_s)*	*Descending time (T_f)*
Below 500 μs	Below 1500 μs	Below 500 μs

2.2.2 Receiver

The receive BER of a mobile RFID is below 0.001%. The threshold receiving level of the antenna in a mobile RFID should be –70 dBm, which is referred to as receive sensitivity. Adjacent channel rejection refers to the difference between interferer level and original signal level, wherein the interferer level is measured when BER falls below 0.001% by inputting the original signal 3 dB higher than receive sensitivity into the channel and increasing the interferer level of the adjacent channel at the same time. Non-adjacent channel rejection refers to the difference between the interferer level and original signal level, wherein the interferer level is measured when BER falls below 0.001% by inputting the original signal 3 dB higher than receive sensitivity into the channel and increasing the interferer level of a non-adjacent channel at the same time.

These adjacent channel rejections and non-adjacent channel rejections characterise the channel selectivity. The mobile RFID receiver should have 0.001% BER channel selectivity below the figures specified in Table 3 in terms of adjacent and non-adjacent channel rejection. According to the density of mobile RFIDs using channels in a certain area, it is classified as a multi-reader or dense-reader environment and each applies different channel selectivity.

Table 3 Channel selectivity of mobile RFID receiver

Environment	*Channel selectivity*	*Channel spacing*	*Remarks*
Multi-reader	5 dBc	1 channel	Channel ±1 adjacent channel
	35 dBc	2 channels	Channel ±2 adjacent channels
	45 dBc	3 channels	Channel ±3 adjacent channels
	55 dBc	4 channels over	Channel ±4 and over channels
Dense-reader	18 dBc	1 channel	Channel ±1 adjacent channel
	47 dBc	2 channels over	Channel ±2 and over channels

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 3. Network configurations for B2C RFID applications are illustrated in Figure 3. 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 hence no need to control multiple readers, but the B2B model has multiple RFID readers and need to control all of them at a middleware host. Second, final service targets are different. For B2C model the final service targets are human beings and for B2B model are business logics, applications and systems. So target contents to be served are different. Online contents such as images, audio music, songs, movies, news, games, information, etc. are provided by the B2C model. But online 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 towards consumers would get more important 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 makes various networking properties for a network entity and each networking property might make different network architectures (Su et al., 2007).

1 EPC network case: A typical RFID network model may refer to the network architecture of EPCglobal as shown in Figure 3 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, Supply Chain Management (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.

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 4 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.

As the network connectivity expands into consumers, new network entities are installed such as RFID Privacy Management Service (RPS), Wireless Application Protocol (WAP)/web server, mobile handset and mobile network infrastructure as shown in Figure 6 where Object Traceability Service (OTS) is the same to EPC-DS, Object Information Service (OIS) to EPC-IS, ODS to ONS, additionally RPS and WAP/web server.

Figure 3 EPC network's configuration

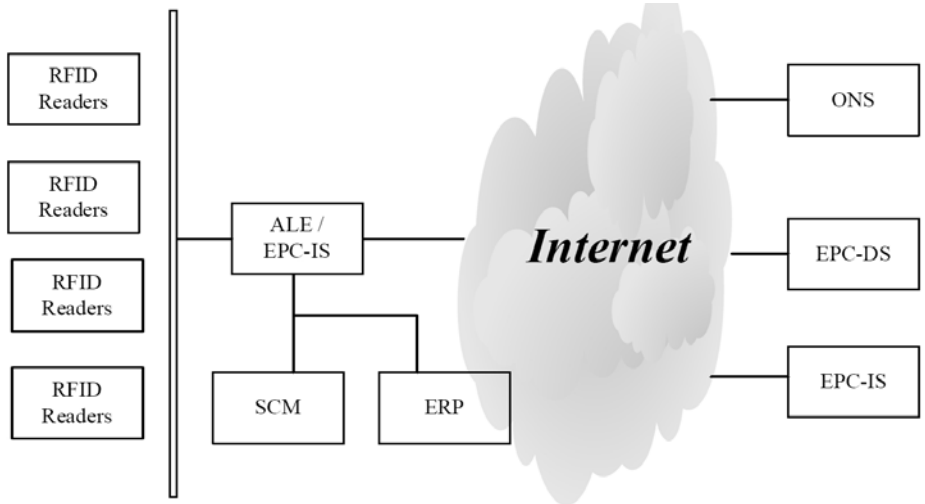
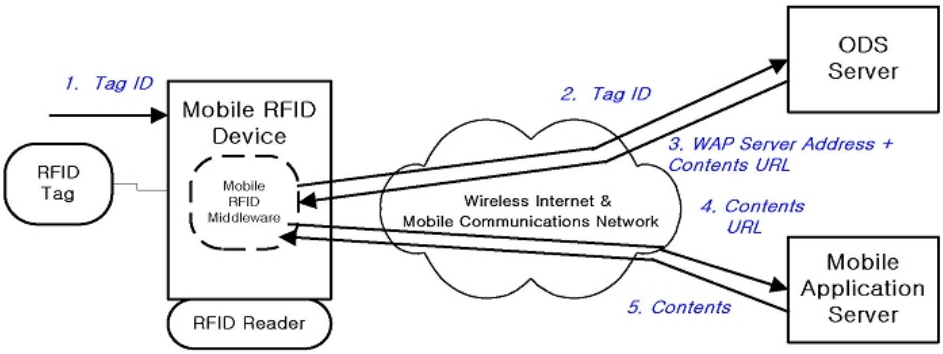


Figure 4 Basic communication model of mobile RFID



2.3.2 Classes of mobile RFID technology

For realisation 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 supports RFID technology based on 13.56 MHz, 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 13.56 MHz complying with ISO/IEC 18092. The Nokia 5140 and 5140i phones as well as 3220 phone with the integrated Xpress-on™ RFID reader shell are 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 metre readings (Nokia, 2004).

KDDI in Japan developed slide-in RFID readers that can be easily attached to the backside 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 315 MHz active type. Some pilot

tests were scheduled in March 2005. Figure 5 shows 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 4 shows a summary of the possible implementations of mobile RFID.

Figure 5 Network architecture model of KDDI's mobile RFID service

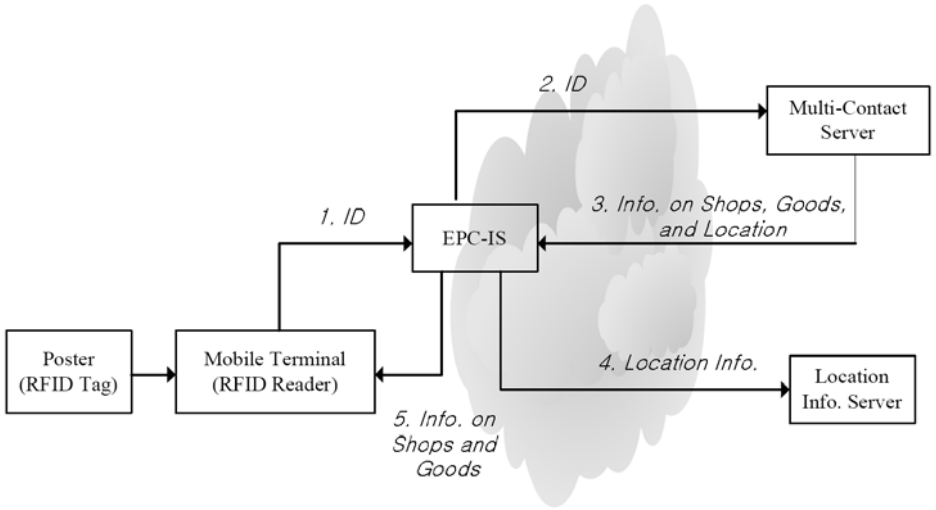


Table 4 Summary of mobile RFID implementations

	Nokia's mobile RFID	*KDDI's mobile RFID (Passive)*	*KDDI's mobile RFID (Active)*	*NFC (Near Field Communication)*	*Korea's mobile RFID*
Radio frequency	13.56 MHz	2.45 GHz	315 MHz	13.56 MHz	860–960 MHz
Reading range	2–3 cm	5 cm	10 cm		
Compliant standards	ISO/IEC 14443A			ISO/IEC 18092	ISO/IEC 18000 6 B/C
Feature	HF RF reader	RF reader	Active RFID reader	Tag and 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 (Chae and Oh, 2005; Garfinkel and Rosenber, 2005; Park et al., 2006a). From the viewpoint of service deployment, the UHF-band is more profitable according to the following observations:

1 It has relatively longer range up to 100 cm.

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

2 *Short range is available up to 2 or 3 cm if required.*

- In the case of the payment system, short range may be supported by reducing the RF strength by application.

3 Avoiding duplicate investment for the RFID tag.

- Most RFID tags in SCM work in the 900 MHz range, that is 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 (e.g. mobile RFID using compact UHF RFID chip in cellular phone) was first attempted in Korea in 2005, their standardisation has been ongoing. Korea's mobile RFID technology is focusing on the UHF range (Park and Lee, 2004; Chae and Oh, 2005; Yoo, 2005). 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.

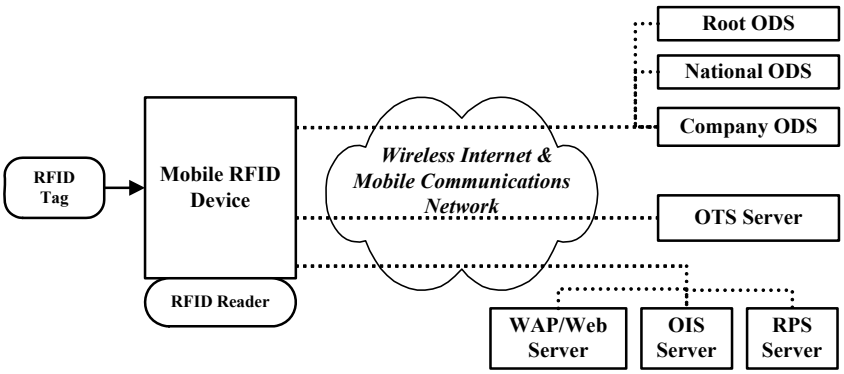
The mobile RFID service has been defined as the provision, through the wireless internet network, of personalised secure services – such as searching for product information, purchasing, verifying and paying for products – while on the move, by building the RFID reader chip into the mobile terminal (Sullivan, 2004; Tsukada and Narita, 2006). 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 6 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/ ANTS (Base Transceiver Station/Access Network Transceiver Subsystem) and wire communication takes place between BTS/ANTS and a networked RFID application server.

Figure 6 represents the entities of the mobile RFID service network architecture. The Object Directory Service (ODS) 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). The role of ODS is same as EPCglobal's ONS. The ODS server plays the role of a DNS server which informs the mobile RFID phone of the contents/service server's location, as explained above (Yoo, 2005; Kim and Koshizuka, 2006; Sakurai and Kim, 2006). The ODS server may be organised in a hierarchical

structure similar to that of a DNS server. The OTS 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 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 and expiration time. The RPS controls access to the information on the object in accordance with the privacy profile put together by the owner of the object. The WAP and web servers are contents servers that provide wireless internet contents such as news, games, music, videos, stock trading, lotteries, images and so forth.

Figure 6 Conceptual network model for mobile RFID service



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 (Chae and Oh, 2005; Sakurai and Kim, 2006; TU-T TSAG, 2006). It will also be possible to mount the RF wireless communication function on the reader chip using Software-Defined Radio (SDR) technology and develop an ISO/IEC 18000-6 A/B/C communication protocol in software to choose from the protocols when needed.

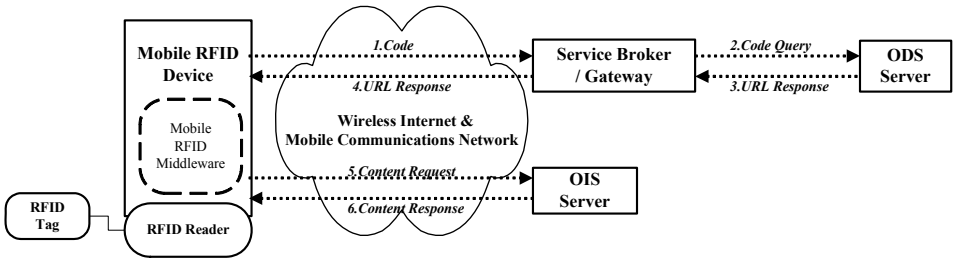
The mobile RFID middleware is composed by extending the Wireless Internet Platform for Interoperability (WIPI) software platform to provide RF code-related information obtained from an RF tag through an RFID reader installed in the mobile phone. The networked terminal's function is concerned with the recognition distance to the RFID reader chip built into the cellular phone, transmission power, frequency, interface, technological standard, Personal Identification Number (PIN) specification, Universal Asynchronous Receiver and Transmitter (UART) 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 (Park and Lee, 2004; Sullivan, 2004; Chug et al., 2005; Kim and Koshizuka, 2006).

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 standardising 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.

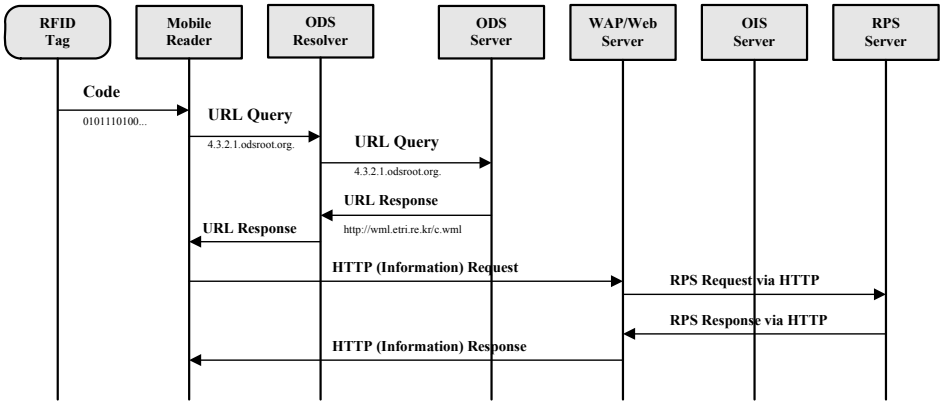
Figure 7 Block basic communication scenario for mobile RFID service



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 (Park and Lee, 2004; Yoo, 2005; Park et al., 2006a). 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 8 as a DNS server 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.

Figure 8 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 (Garfinkel and Rosenberg, 2005; Yoo, 2005; Mobile RFID Forum of Korea, 2005c; Lee and Kim, 2006). Given that '1.2.3.4' is obtained from a bit string translation and that '1.2.3.4' should be converted into a Uniform Resource Name (URN) 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.

Figure 8 Detailed mobile RFID's code resolution process



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 section 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 online contents and services with unique code structures suitable for mobile RFID service.

3.3 Mobile RFID code structure registration

The top registration organisation in charge of TLC allocation is needed for comprehensive and efficient management of the code system. The upper provider that is assigned TLC takes charge of allocating Company Code (CC). The upper provider decides which class code to give to the service provider asking for code allocation, depending on the number of needed identifiers and substructure.

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 section, 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 consists 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 centre has defined five classes based on functionality (Sarma et al., 2002; Yoo, 2005).

Table 5 RFID tag functionality classes

Class	*Nickname*	*Memory*	*Power source*	*Features*
0	Anto-shoplift tags	None	Passive	Article sureveillance
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 the 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, handheld 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 (Weis et al., 2003).

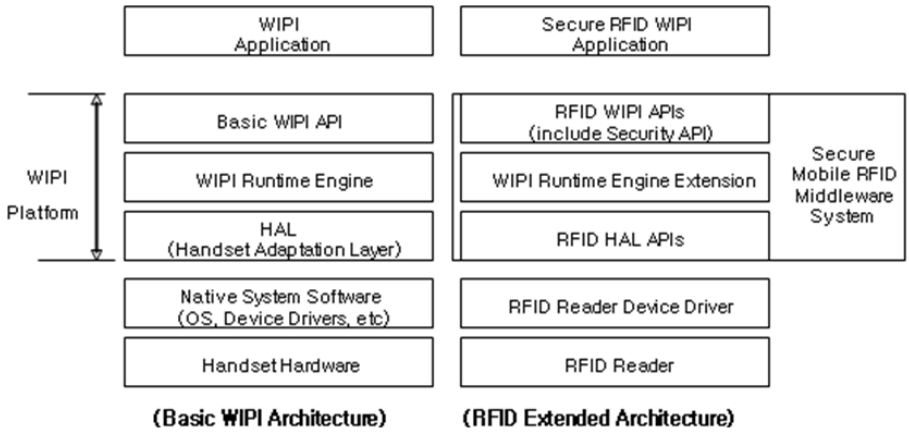
Figure 9 The mobile RFID reader (see online version for colours)

4.2 Mobile terminal platform for networked RFID

4.2.1 Conceptual view of mobile RFID middleware platform

One of the key problems with mobile RFID technology is how to quickly use the mobile RFID reader and its integration with the application software installed on the mobile device. In the face of numerous existing types of application software, developing an independent mobile RFID middleware layer presents a promising alternative. The mobile RFID middleware layer inhabits the middle ground between the RFID reader and the application logic layer (Finkenzeller, 2003). 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 a middleware platform used in South Korea that allows mobile phones, regardless of manufacturer or carrier, to run applications. WIPI supports the interoperability platform for various application software and hardware platforms (Sullivan, 2004). Therefore, we chose WIPI as the basic software development platform of the mobile phone: the software architecture and the relationship between each of the software functions are shown in Figure 10.

Figure 10 Architecture of RFID extended mobile embedded platform



The software architecture is composed of REX OS, WIPI HAL (Handset Adaptation Layer) API, WIPI Runtime Engine (WRE), WIPI C API, phone application, browser parser and phone GUI. Most functions for mobile RFID technology are designed in the WIPI C API: they are reader control, tag control, buffer control and filter control for interfacing with the RFID reader; and code decoder, URN converter, Fully Qualified Domain Name (FQDN) 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 and 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

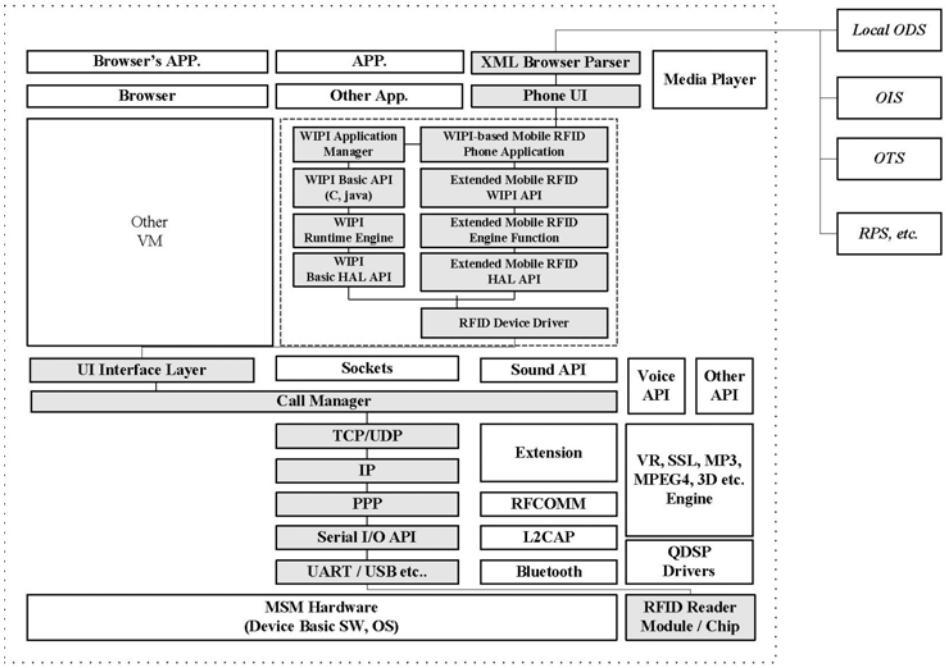
requirements to the handset vendors whether they accept it or not. For example, the run time engine part is required as the mode of download of binary code for its maximum performance. The core functions of the WIPI are the handset adaptation and APIs which are called 'HAL' and 'Application Adaptation 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 supports the C/C++ and Java programming languages. The AAL provides the definitions for functions of adaptive functions for RFID engine, C/Java API, crypto libraries and RFID security components.

Mobile RFID middleware is composed by extending the WIPI software platform to provide RF code-related information obtained from an RF tag through an RFID reader installed in the mobile phone. The functions of enhanced RFID WIPI C API include RFID reader control, buffer control, tag control, filtering, networking for code decoding, URN conversion, FQDN conversion, DNS resolving and the content services.

WIPI Runtime Engine software for mobile RFID functions is extended to support RFID WIPI C API and RFID HAL API. The functions of RFID HAL API include RFID reader control, buffer control, tag control, filtering and networking for configuring the Internet Protocol (IP) address of the local ODS server. Figure 11 shows the middleware functions and software.

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 specification, UART communication interface, WIPI API extended specification to control the reader chip.

Figure 11 Block diagram of the mobile platform for networked RFID



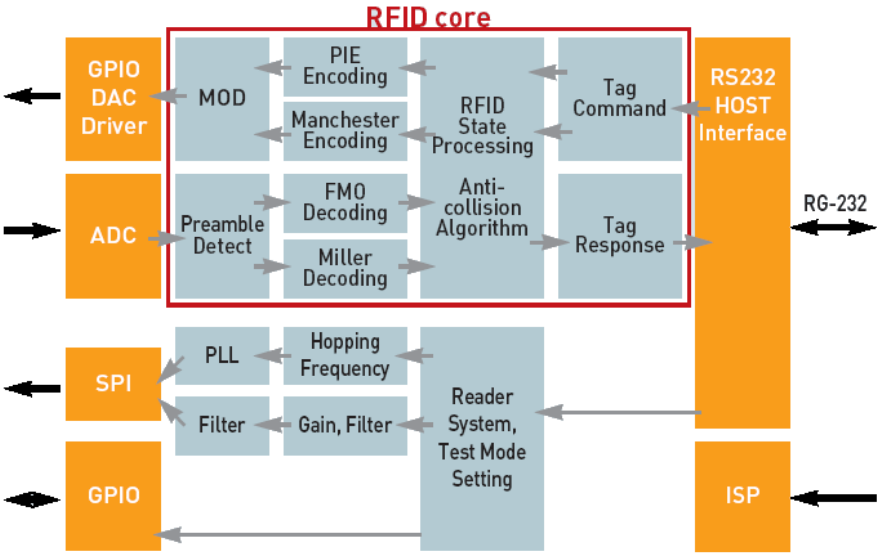
RFID reader chip middleware functions are provided to the application program in the form of mobile platform's API. Here, the mobile RFID device driver is the device driver software provided by the reader chip manufacturer. The RFID device handler provides the definitions for functions of starting the platform and transferring the events from the upper layer of HAL to the RFID H/W reader.

4.2.2 UHF-banded mobile RFID H/W reader

UHF mobile RFID reader is a handheld 900 MHz RFID reader and can be used as a peripheral of the mobile devices such as a cellular phone, smart phone and PDA. Its compatibility of EPC C1G2 and the capability of wireless communication provide many possible applications.

For a mobile terminal with an RFID reader embedded, the configuration of reader chip and adjacent circuitry can be illustrated, as shown in Figure 12. Inside the reader chip are two components: the digital component, which processes host/RFID protocols; and the analogue component, which processes baseband signals and 900 MHz RF signals. Our reader 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.

Figure 12 Block diagram of the UHF band mobile RFID reader (see online version for colours)



4.2.3 Data processing using middleware platform

In this section, we design a mobile RFID middleware to support trust and secure m-business based on RFID. The mobile RFID terminal is a function which is concerned with the recognition distance to the RFID reader chip built into the cellular phone, transmission power, frequency, interface, technological standard, PIN specification,

UART communication interface, WIPI API and WIPI HAL API extended specification to control reader chip. RFID reader chip middleware functions are provided to the application program in the form of WIPI API as shown in Figure 13. Here, 'mobile RFID device driver' is the device driver software provided by the reader chip manufacturer. The mobile RFID network function is concerned with the communication protocols such as the ODS communication for code interpretation, the message transmission for the transmission and reception of contents between the cellular phone terminal and the application server, contents negotiation that supports mobile RFID service environment and ensures the optimum contents transfer between the cellular 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 extended specification which supports these communication services. The mobile RFID middleware is implemented by extending the WIPI platform to provide RF code-related information obtained from the RF tag through the RFID reader installed in the mobile phone (Mobile RFID Forum of Korea, 2005a, Mobile RFID Forum of Korea, 2005e; Park et al., 2006c; Park et al., 2006d). The functions of RFID WIPI C API include RFID reader control, buffer control, tag control, filtering, networking for code decoding, URN conversion, FQDN conversion, DNS resolving and the content services.

1 *Mobile RFID code resolution function*: Figure 14 shows middleware functions and software architectures overall. WIPI platform has been set to minimise the side effect that may occur due to the use of various platforms. Before the mobile phone communicates with legacy networks we have to resolve bit string codes to obtain the URN by code decoder and URN converter sub-functions as shown in Figure 14 and the code resolution function is depicted in Figure 14 (Son et al., 2006). To discover a contents server we communicate with local ODS server via FQDN converter and DNS resolver sub-functions as depicted in Figure 14. After phone application receives the response message it extracts the URL of contents server from it. To download browsing information we connect to the contents server through connect content server sub-function depicted in Figure 13 on the HTTP/TCP/IP protocol stack. The code resolution function is depicted in Figure 13. Local ODS server is a DNS server using UDP port 53 and contents server is a web server using TCP port 80 for HTTP.

2 *Function scenario in mobile RFID middleware*: In scenario, a mobile RFID client performs an update for its own middleware in the security server, where applying security modules to implement business processes satisfies security requirements. In this scenario, an RFID service provider already been authenticated can do 1-to-N businesses (from one provider to multiple providers) as well as 1-to-1 business (from one provider to one provider), because she/he can search and access to various RFID middleware registered in the RFID security server. To offer more flexible access to multiple business providers, distributed registries need to be integrated, but it causes the problems of user authentication and security vulnerability. By applying single sign on scheme, we can simplify user authentication and overcome the problems. The detailed function are as follows (Figure 15) (Mobile RFID Forum of Korea, 2005d; Mobile RFID Forum of Korea, 2005f).

Figure 13 Function block diagram of mobile RFID middleware platform in the mobile phone

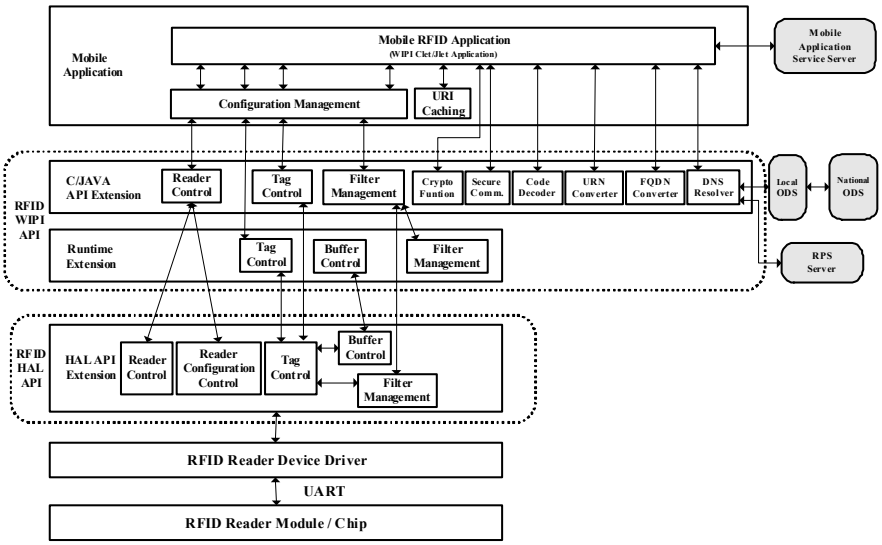


Figure 14 Code resolution flow chart based on mobile RFID middleware

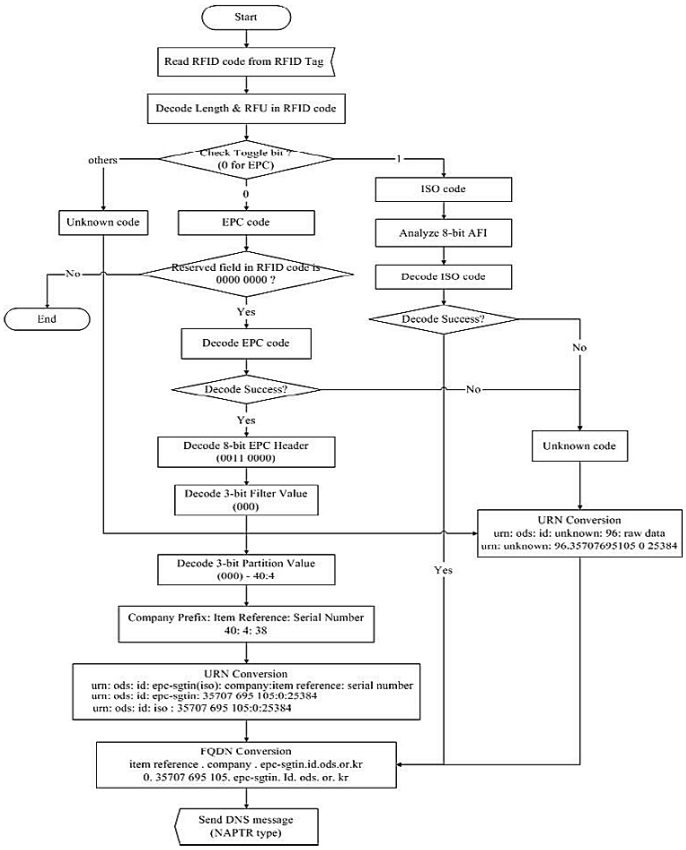
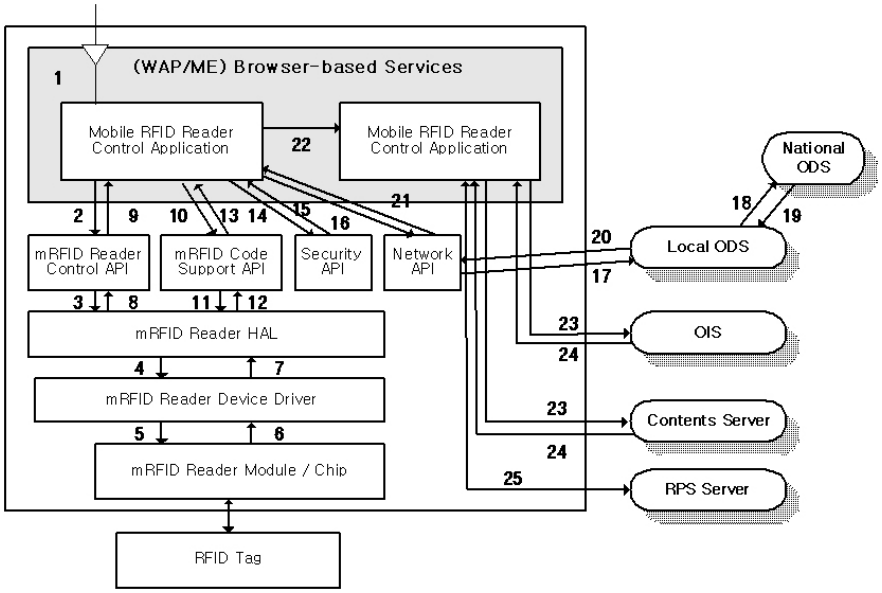


Figure 15 Scenario of secure mobile RFID M/W terminal function



- RFID reader module/chip: the RFID reader module or chip-type hardware mounted or built into to the cellular phone RFID
- Reader device driver: system software to provide RFID reader device control
- RFID reader HAL: HAL to retain the hardware independence to RFID reader
- RFID reader control API: API to enable application to control RFID reader
- RFID code-support API: API to enable the application to interpret the information read from RFID tag or convert the information to save
- Network API (embedded for RFID): API to enable the application to access ODS using the information read from the RFID tag and OIS to obtain related information
- Security API (embedded for RFID): API to give the application for various security functions required when communicating with RFID tag or ODS, OIS, contents server
- RFID reader control application: Application built into the cellular phone to control RFID reader and reads the RFID tag and inter-works with WAP or ME (Mobile Exploerer) browser with the information read
- RFID custom application: Application downloaded to the cellular phone to read RFID tag and provide services according to the information read.

The detailed message communication processes are as follows.

1 The user clicks the application is the button or starts the RFID reader application from the cellular phone is the application menu.

2 Application calls RFID reader control API.

3 RFID reader calls HAL API.

4 Transmits the command to RFID reader is device driver.

5 Transmits the command to RFID reader to start reader.

6 Obtains the result from the reader.

7 Device driver returns RFID reader results to HAL.

8 HAL returns the RFID reader results to reader control API.

9 Reader control API returns the RFID reader results to application.

10 Application calls RFID code-support API to interpret the RFID tag data code.

11 Code-support API calls HAL API for common memory access of the handheld terminal to interpret the code.

12 HAL returns the common memory access data to code-support API.

13 Code-support API interprets the tag data code read based on the code in the common memory contents and transmits the result to the application.

14 If the tag represents adult level, calls the security API for service authorisation.

15 The result of authorisation for adult service to the application.

16 Creates ODS question message by extracting the required codes through the code interpretation from (Park et al., 2006) and calls network API.

17 Requests local ODS for the URI related to the code extracted from (14) above through network API. (This type of network API is referred to as ODS resolver)

18 If local ODS does not have the OIS information or contents server information related to the transmitted code, it sends the transmitted code to national ODS to request such information.

19 National ODS transmits the URI related to the transmitted code to local ODS.

20 Local ODS returns the transmitted URI to network API.

21 Network API returns this to application.

22 The application runs WAP/ME browser using the URI acquired.

23 WAP/ME browser accesses the OIS or contents server using the URI acquired to request for tag related information.

24 OIS or contents server transmits the product or service protocol related to the OID of the transmitted tag so that WAP/ME browser can display it on the screen.

25 Let the user determines the privacy level by displaying the policy configuration screen for the required privacy in the middle of the communication with OIS or contents server when privacy protection is required.

Secure mobile RFID middleware terminal platform system has been implemented based on the design described in previous section. By applying suggested mobile RFID middleware terminal platform to system framework and mobile RFID service as shown in Figure 16.

Figure 16 Proposed secure mobile RFID middleware's development (see online version for colours)

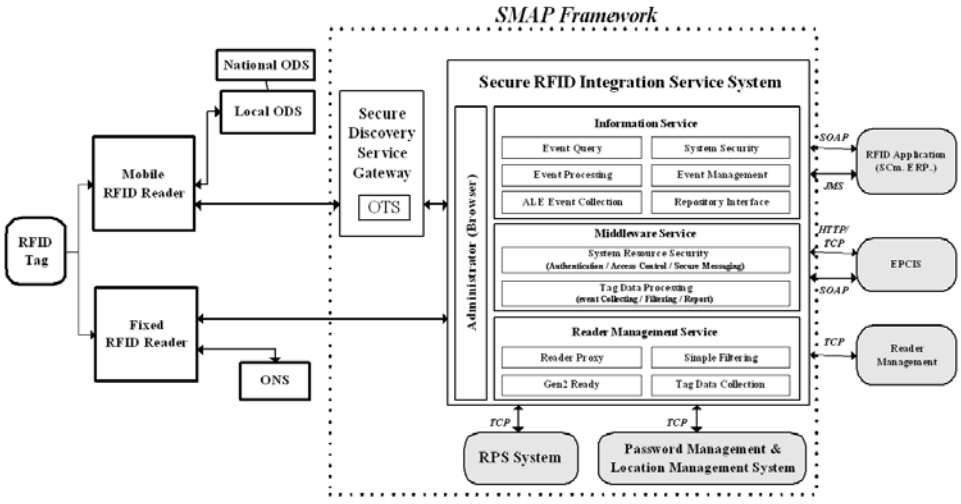
4.3 Back end service system

4.3.1 Portal discovery service gateway

In phone-based networked RFID, we propose gateway system that is capable of managing the OIS server, enhancing the security and privacy, managing the service applications, etc. These features make efficient phone-based networked RFID applications on the network. The gateway system helps the RFID application easily connects the OIS server to get product information and service information regarding to the RFID code. It means that the gateway system provides the traceability for a specific product. Also, it has OIS server management capabilities such as database management of the OIS server and synchronisation of the data between the servers.

Another feature of the gateway is that it provides the security and privacy enhancing features to the RFID application. Access control mechanism, authentication and code recoding are also provided by this gateway system. The gateway provides the authentication and authorisation method to the RFID application correspondents. Only the authorised user can access the OIS server and gets the contents of the code. Password and certificate-based authorisation methods, which is based on the X.509, are provided in this system.

Figure 17 Arch. of portal discovery service gateway system



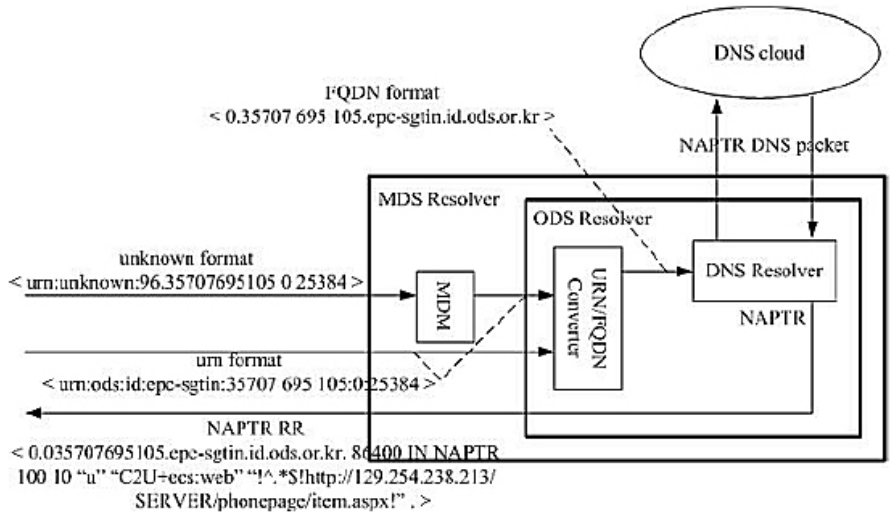
The gateway provides the privacy protection method to the RFID user by making the RFID tag with personalised one. By changing the original code value into new one, only the user who knows the original code value can get the contents of the tag. The gateway system manages code recoding technique by managing the lookup table of the code values. In this case, only the authorised user can access the lookup table. The privacy enhancing capability is due to our proposed mechanism, so called the RFID Privacy Service (RPS). This mechanism is in the process of international standardisation at ITU-T (Park and Lee, 2004). The RPS mainly consists of three components such as Privacy Profile Processing (PPP) controller, which controls the main operation of RPS, RPS decision agent, which adapts the privacy and audit policy profile to all RFID participants and decides the level of security in each transactions, OIS schema manager, which manages and updates the schema values of the RPS.

4.3.2 ODS 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 18, consists of the Multicode Decoding Module (MDM), 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 (Son et al., 2006).

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.

Figure 18 Local ODS server system functions



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 related 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 (Park et al., 2005; Park et al., 2007).

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.

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, desktop PC and business systems for logistics and 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.

Content negotiation: A mobile phone has a variety of software operation environments. They involve screen size and shape, resolution, colour, software implementation platform, browser, input/output interface, 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 favourite 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 application

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 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 ARP. 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, such as application service requirements, code system requirements, RFID tag requirements, RFID reader requirements, test requirements, network environment requirements and security requirements, for the mobile RFID services.

5.1 Mobile RFID service range

1 *Frequency conditions*: The mobile RFID service standard supports only 900 MHz UHF communication based on the ISO/IEC 18000-6. That is, mobile RFID reader chips and tags are communication devices working in the 900 MHz frequency range. According to the ISO/IEC 18,000 standard, radio frequencies for RFID applications are as shown in Table 6.

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 *Online 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 900 MHz 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 900 MHz reader chip and WIPI platform, the mobile RFID services would be accessible under the WIBRO mobile internet communication environment.

Table 6 ISO/IEC 18000-x wireless access standard

Specification	*Description*
ISO/IEC 18000-1	Reference architecture and definition of parameters to be standardised
ISO/IEC 18000-2	Parameter for air interface communication below 135 kHz
ISO/IEC 18000-3	Parameter for air interface communication at 13.56 MHz
ISO/IEC 18000-4	Parameter for air interface communication at 2.45 GHz
ISO/IEC 18000-5	Parameter for air interface communication at 860 <MHz to 960 MHz
ISO/IEC 18000-6	Parameter for active air interface communication at 433 MHz

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 related 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 centre. 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 recognise through a mobile phone that has a limited data input/output environment (Mobile RFID Forum of Korea, 2005c).

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 organisations 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 requirement 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 analysing secure mobile RFID service models to solve security issues like security among domains, personal privacy profile, authentication, end-to-end security and track prevention (Yutaka and Nakao, 2002; Kwak et al., 2005; Konidala and Kim, 2006; Lee and Kim, 2006).

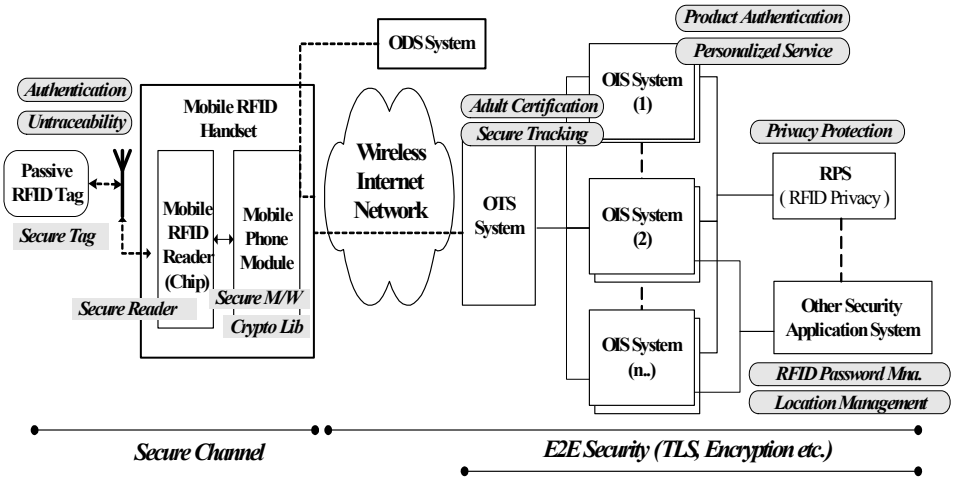
There are many ways to interfere with RFID circumstances, issues which are not only approved theoretically but also possible practically. Besides security vulnerabilities in RFID security like passive signal interception attack on RFID tags and readers, reading of RFID tags by unauthorised readers, falsifying tag or reader identity, use of attack tools against RFID tags, neutralisation 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, some information protection service models are needed 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 section suggests and analyses 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.

6.1 Security service framework

RFID data privacy may be compromised in various ways, using methods that have been proven not only theoretically but also practically. RFID vulnerabilities such as passive signal interception, unauthorised scanning, falsifying tag or reader identity, use of attack tools against RFID tags, deactivation of RFID tags and elaborate attacks involving cryptographic hacking are all possible with mobile RFID readers. Furthermore, information protection service models are needed that ensure security and privacy and management for service providers in practical compliance with present RFID specifications and mobile RFID standards, even when tags do not use code algorithms.

For this purpose, the author developed a mobile RFID protection policy named MRF-Sec631 (Mobile RFID-Security 6.3.1) together with the proposed mobile RFID information protection service model. Specifically speaking, MRF-Sec631 supports six typical security functions for mobile RFID readers, provides three main security service mechanisms and the execution of secure mobile RFID services through application portal services. The six security functions provided by the API are data encryption, secure communication, key management, EPC Class 1 Gen2 security command, adult certification and privacy protection. The three security service mechanisms are authentication, privacy protection and secure location tracking. The one-secure application service is secure mobile RFID application portal service (Garfinkel et al., 2005; MIC of Korea, 2005; Thornton et al., 2006; Choi et al., 2007).

Figure 19 Conceptual architecture of secure mobile RFID service framework



The main functions of the proposed service model are the provision of WIPI-based mobile security middleware, tag authentication, tag tracking prevention, reader authentication, message security, non-traceable payment and policy-based privacy protection (Ohkubo et al., 2003; Mobile RFID Forum of Korea, 2005a; Park, 2008).

6.2 Multilateral approaches for improved privacy

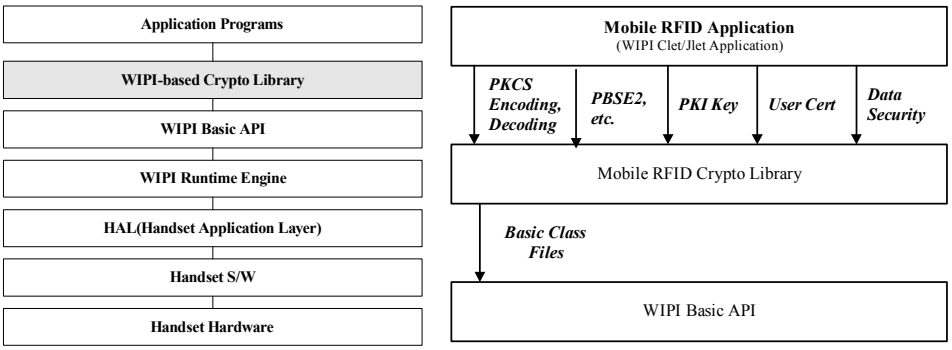
We adopt a threefold approach to system design, with security mechanisms on the platform, protocol and privacy levels. At the platform level, the system consists of an

application portal, IS server, reader security application, payment server and privacy protection server. It provides a combined environment to facilitate building a mobile RFID security application service. At the protocol level, both write and kill command passwords provided by EPC Class 1 Gen2 are used to 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. And at the privacy level, random acquisition of tag information by unauthorised readers is prevented. 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 set policies that allow authorised persons complete access but limit or completely restrict access to unauthorised persons (Park et al., 2006e; Prabhu et al., 2006; Park, 2010).

6.3 Robust encryption in middleware platform

The mobile RFID middleware is the key enabling infrastructure that leverages existing investments and new development in security standards to bring robust mobile RFID's terminal platform security in the enterprise. When selecting a suitable mobile RFID service system, consideration should be given to crypto logical functions. Applications that do not require a security function would be made unnecessarily expensive by the incorporation of crypto logical procedures. On the other hand, in high security applications (e.g. mobile ticketing, payment systems) the omission of crypto logical procedures can be a very expensive oversight if manipulated mobile RFID readers are used to gain access to services without authorisation (Shepard, 2005; Park and Song, 2010a; Park, 2011).

Figure 20 Architecture crypto library in mobile middleware



Below is the method of reinforcing RFID data communication security service by using crypto algorithm based on mobile phone terminal platform in mobile RFID service. The mobile RFID crypto library is a crypto library for the efficient processing of the crypto algorithms and security protocols. It provides security mechanisms to the mobile RFID reader and targets the mobile RFID middleware based on the WIPI platform. The mobile

RFID crypto library enables the mobile RFID service provider, wireless contents provider and information security industry to support the information protection service on the mobile RFID middleware terminal platform at a reasonable cost and in a short period of time (Park et al., 2006b; Park et al., 2008; Park and Gadh, 2010; Park and Kim, 2010; Park and Song, 2010b).

Its main features are crypto algorithms (AES, DES, 3DES, SHA-1, HAS160, HMAC, etc.), high speed Elliptic Curve Cryptosystem (ECC) and digital signature (ECC, ECDSA, etc.), high speed Korean standard crypto algorithms and digital signature (SEED, KCDSA, ARIA, etc.), secure communication protocol (SSL/TLS, etc.), and public key crypto standard (PKCS #5, PKCS #8 , ASN.1, etc.). Crypto logical procedures are used to protect against both passive and active attacks. To achieve this, the transmitted data (plain text) can be altered (encrypted) prior to transmission so that a potential attacker can no longer draw conclusions about the actual content of the message (plain text). The mobile RFID systems have for a long time used only symmetrical procedures. Because block ciphers are generally very calculation intensive, they play a less important role in mobile RFID service systems.

The mobile RFID's crypto algorithm library has been implemented based on the design described in previous contents. Figure 21 represents test bed architecture of library component. We use test bed system of WIPI and J2ME (Java 2, Micro Edition) environment to simulate the processing of various service protocols. J2ME is a set of technologies and specifications developed for small devices like smart cards, pagers, mobile phones and set-top boxes. J2ME uses subset of Java 2, Standard Edition (J2SE) components, like smaller virtual machines and leaner APIs. J2ME has categorised wireless devices and their capabilities into profiles: MIDP, PDA and Personal. Mobile Information Device Profile (MIDP) and PDA profiles are targeted for handhelds and personal profile for networked consumer electronic and embedded devices. As the technology progresses in quantum leaps any strict categorisation is under threat to become obsolete. It is already seen that J2ME personal profiles are being used in high-end PDAs such as pocket PCs and mobile communicators. We will concentrate on the most limited category of wireless J2ME devices that use MIDP. Applications that these devices understand are Clets and Midlets. Midlet is a JAR (Java Archive) archive conforming to the Midlet content specification. Figure 22 shows an example of the crypto algorithm development in mobile RFID terminal platform environment.

Figure 21 Service structure of mobile RFID crypto library

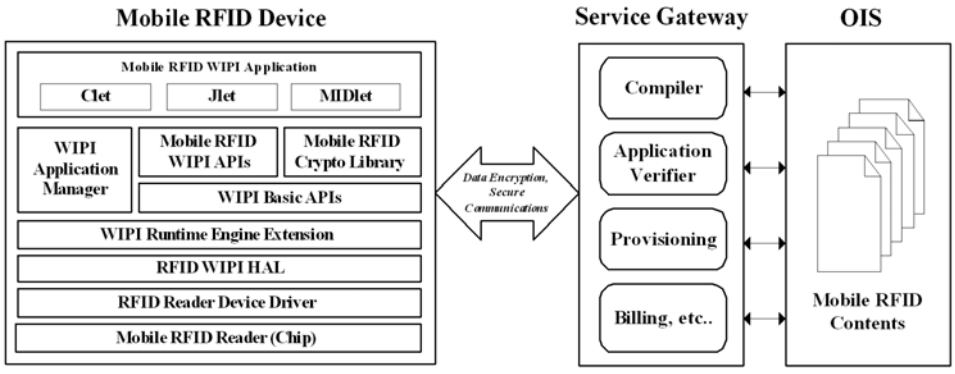


Figure 22 Crypto algorithm's GUI in mobile RFID middleware (see online version for colours)

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 section, 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 908.5 MHz to 914 MHz in Korea in order to comply with ISO 18000-6 for air interface communications at 860 MHz to 960 MHz. 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 900 MHz) 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, customised 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.

References

Avoine, G. and Oechslin, P. (2005) 'RFID traceability, a multilayer problem', in Patrick, A. and Yung, M. (Eds): *Financial Cryptography – FC'05*, Vol. 3570, Springer-Verlag, Berlin, Heidelberg, pp.125–140.

Chae, J. and Oh, S. (2005) *Information Report on Mobile RFID in Korea*, ISO/IEC JTC1/SC 31/WG4 N0922, Information paper, ISO/IEC JTC1 SC31 WG4 SG 5.

Choi, D., Kim, H. and Chung, K. (2007) *Proposed draft of X.rfidsec-1: privacy protection framework for networked RFID Services*, ITU-T, COM17C107E, Q9/17, Contribution 107, Geneva.

Chug, B. et al. (2005) 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.

Finkenzeller, K. (2003) RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification, Wiley, Chichester, UK.

Garfinkel, S., Juels, A. and Pappu, R. (2005) 'RFID privacy: an overview of problems and proposed solutions', *IEEE Security and Privacy*, Vol. 3, No. 3, pp.34–43.

Garfinkel, S. and Rosenberg, B. (2005) *RFID: Applications, Security, and Privacy,* Addison-Wesley, Upper Saddle River,

ITU-T TSAG (2006) RFID CG Deliverable Review Report of Identification Based Business Models and Service Scenarios, ITU-Telecom.

Kim, Y. and Koshizuka, N. (2006) Review Report of Standardization Issues on Network Aspects of Identification Including RFID, ITU-T, Paper TD315.

Kim, Y., Lee, J., Yoo, S. and Kim, H. (2006) 'A network reference model for B2C RFID applications', *Proceedings of 8th ICACT*, 20–22 February, 4p.

Konidala, D.M. and Kim, K. (2006) 'Mobile RFID security issues', *Proceedings of Symposium on Cryptography and Information Security*, Hiroshima, Japan.

Kwak, J., Rhee, K., Oh, S., Kim, S. and Won, D. (2005) 'RFID system with fairness within the framework of security and privacy', *Lecture Notes in Computer Science*, Vol. 3813, pp.142–152.

Lee, B., Kim, H. and Chung, K. (2006) 'The design of dynamic authorization model for user centric service in mobile environment', *Proceedings of 8th International Conference on Advanced Communication Technology (ICACT 2006)*, 20–22 February, Vo1. 3.

Lee, H. and Kim J. (2006) 'Privacy threats and issues in mobile RFID', *Proceedings of the 1st International Conference on Availability, Reliability and Security,* Vol. 1, pp.510–514.

Lee, J. and Kim, H. (2006) 'RFID code structure and tag data structure for mobile RFID services in Korea', *Proceedings of the 8th International Conference ICACT*, Vol. 2, 20–22 February, 3p.

MIC (Ministry of Information and Communication) of Korea (2005) *RFID Privacy Protection Guideline*, MIC Report Paper.

Mobile RFID Forum of Korea (2005a) *Access Right Management API Standard for Secure Mobile RFID Reader, MRFS-4-03*, Standard Paper. Available online at: http://www.mrf.or.kr

Mobile RFID Forum of Korea (2005b) *HAL API Standard for RFID Reader of Mobile Phone*, Standard Paper.

Mobile RFID Forum of Korea (2005c) *Mobile RFID Code Structure and Tag Data Structure for Mobile RFID Services*, Standard Paper. Available online at: http://www.mrf.or.kr

Mobile RFID Forum of Korea (2005d) *WIPI API for Mobile RFID Reader Device*, Standard Paper.

Mobile RFID Forum of Korea (2005e) *WIPI C API Standard for Mobile RFID Reader*, Standard Paper.

Mobile RFID Forum of Korea (2005f) *WIPI Network APIs for Mobile RFID Services*, Standard Paper.

Nokia (2004) *RFID Phones – Nokia Mobile RFID Kit*. Available online at: http://europe.nokia.com

Ohkubo, M., Suzuki, K. and Kinoshita, S. (2003) *Cryptographic Approach to 'Privacy-Friendly' Tags*, RFID Privacy Workshop, MIT, MA, USA.

Park, B., Lee, S. and Youm, H. (2006a) *A Proposal for Personal Identifier Management Framework on the Internet*, ITU-T, COM17-D165, Geneva.

Park, N. (2008) Reliable System Framework Leveraging Globally Mobile RFID in Ubiquitous Era, PhD Thesis, Sungkyunkwan University, South Korea.

Park, N. (2010) 'Security scheme for managing a large quantity of individual information in RFID environment', *Communications in Computer and Information Science (CCIS)*, Vol. 106, pp.72–79.

Park, N. (2011) 'Secure UHF/HF dual-band RFID: strategic framework approaches and application solutions', *Lecture Notes in Computer Science*, Vol. 6922, pp.488–496.

Park, N. and Gadh, R (2010) 'Implementation of cellular phone-based secure light-weight middleware platform for networked RFID', *28th International Conference on Consumer Electronics (ICCE)*, pp.495–496.

Park, N. and Kim Y. (2010) 'Harmful adult multimedia contents filtering method in mobile RFID service environment', *Lecture Notes in Artificial Intelligence*, Vol. 6422, pp.193–202.

Park, N., Kim, H., Chung, K. and Sohn, S. (2006b) 'Design of an extended architecture for secure low-cost 900 MHz UHF mobile RFID systems', *IEEE Tenth International Symposium on Consumer Electronics (ISCE 2006)*, pp.1–6.

Park, N., Kim, H., Kim, S. and Won, D. (2005) 'Open location-based service using secure middleware infrastructure in web services', in Gervasi, O., Gavrilova, M.L., Kumar, V., Laganá, A., Lee, H.P., Mun, Y., Taniar, D. and Tan, C.J.K. (Eds): *ICCSA 2005: LNCS*, Vol. 3481, Springer, Heidelberg, pp.1146–1155.

Park, N., Kim, S. and Won, D. (2007) 'Privacy preserving enhanced service mechanism in mobile RFID network', *Advances in Soft Computing*, Vol. 43, pp.151–156.

Park, N., Kim, S., Won, D. and Kim, H. (2006c) 'Security analysis and implementation leveraging globally networked mobile RFIDs', *Lecture Notes in Computer Science*, Vol. 4217, pp.494–505.

Park, N., Kwak, J., Kim, S., Won, D. and Kim, H. (2006d) 'WIPI mobile platform with secure service for mobile RFID network environment', *Lecture Notes in Computer Science*, Vol. 3842, pp.741–748.

Park, W. and Lee, B. (2004) Proposal for Participating in the Correspondence Group on RFID in ITU-T, Information Paper, ASTAP Forum.

Park, N., Lee, H., Kim, H. and Won, D. (2006e) 'A security and privacy enhanced protection scheme for secure 900 MHz UHF RFID reader on mobile phone', *IEEE 10th International Symposium on Consumer Electronics (ISCE 2006)*, pp.1–5.

Park, N. and Song, Y. (2010a) 'AONT encryption based application data management in mobile RFID environment', *ICCCI 2010: LNAI*, Vol. 6422, pp.142–152.

Park, N. and Song, Y. (2010b) 'Secure RFID application data management using all-or-nothing transform encryption', *WASA 2010: LNCS*, Vol. 6221, pp.245–252.

Park, N., Song, Y., Won, D. and Kim, H. (2008) 'Multilateral approaches to the mobile RFID security problem using web service', in Zhang, Y., Yu, G., Bertino, E. and Xu, G. (Eds): *APWeb 2008: LNCS*, Vol. 4976, pp.331–341.

Prabhu, B.S., Su, X., Ramamurthy, H., Chu, C-C. and Gadh, R. (2006) 'WinRFID – a middleware for the enablement of radio frequency identification (RFID) based applications', in Shorey, R., Choon, C.M., Tsang, O.W. and Ananda, A. (Eds): *Mobile, Wireless and Sensor Networks : Technology, Applications and Future Directions*, John Wiley & Sons, Inc., New York, pp.331–336.

Sakurai, Y. and Kim, H-J. (2006) Report for Business Models and Service Scenarios for Network Aspects of Identification (Including RFID), ITU-T, TSAG TD 314.

Sarma, S.E., Weis, S.A. and Engels, D.W. (2002) *RFID Systems, Security and Privacy Implications*, Technical Report MIT-AUTOID-WH-014, AutoID Center, MIT.

Shepard, S. (2005) *RFID: Radio Frequency Identification*, McGraw-Hill, New York.

Son, M., Lee, Y. and Pyo, C. (2006) 'Design and implementation of mobile RFID technology in the CDMA networks', *Proceedings of 8th International Conference of Advanced Communication and Technology, (ICACT)*, 20–22 February, 4p.

Strandburg, K.J. and Raicu, D.S. (2005) Privacy and Technologies of Identity: A Cross-disciplinary Conversation, Springer, New York.

Su, X., Chu, C-C., Prabhu, B.S. and Gadh, R. (2007) 'On the identification device management and data capture via WinRFID edge-server', *IEEE Systems Journal*, Vol. 1, No. 2, pp.95–104.

Sullivan, L. (2004) *Middleware Enables RFID Tests*, Information week, Vo. 991.

Thornton, F., Haines, B., Das A.M., Bhargava, H. and Kleinschmidt, J. (2006) *RFID Security*, Syngress Publishing Inc., Rockland, MA.

Tsuji, T., Kouno, S., Noguchi, J., Iguchi, M., Misu, N. and Kawamura, M. (2004) 'Asset management solution based on RFID', *NEC Journal of Advanced Technology*, Vol. 1, No. 3, pp.188–193.

Tsukada, M. and Narita, A. (2006) 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.

TU-T TSAG (2005) A Proposed New Work Item on Object/ID Associations.

Weis, S., Sarma, S.E., Rivest, R.L. and Engels, D.W. (2003) 'Security and privacy aspects of low-cost radio frequency identification systems, *Proceeding of 1st International Conference on Security in Pervasive Computing*, pp.201–212.

Yoo, S. (2005) *Mobile RFID Activities in Korea*, Contribution Paper of the APT Standardization Program.

Yutaka, Y. and Nakao, K. (2002) A Study of Privacy information Handling on Sensor Information Network, Technical report of IEICE.