>P5-14<

Implementation of Cellular Phone-based Secure Light-Weight Middleware Platform for Networked RFID

Namje Park and Rajit Gadh

UCLA-WINMEC, Los Angeles, USA

Abstract — *We describe the core components of a mobile RFID system, and they include components such as mobile RFID reader, platform architecture and network architecture. Although there are several kinds of mobile RFID readers in the market, we will propose specially designed mobile RFID technology which has several positive features including security features, network architecture, operation scenario, and, code resolution mechanism. We will analyze the characteristics of the proposed technologies.*

I. INTRODUCTION

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 [2]. 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 (Wireless Internet Platform for Interoperability) 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 [3]. 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 as figure 1.

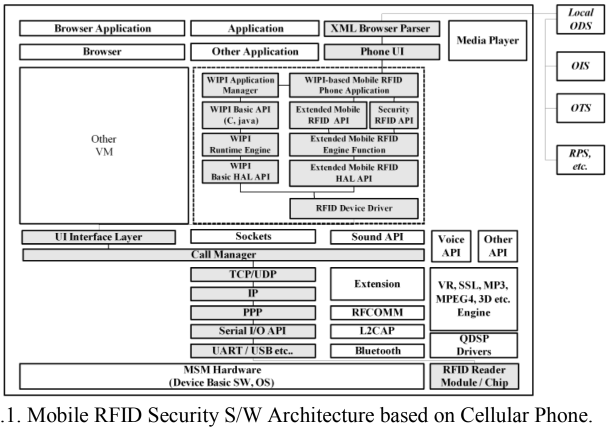

Fig.1. Mobile RFID Security S/W Architecture based on Cellular Phone.

The software architecture is composed of REX OS, WIPI HAL 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, FQDN(Fully Qualified Domain Name) converter, DNS resolver and connect contents server for communicating with a local ODS server and the contents web server.

In the WIPI specifications, the core functions are the functions of the handset hardware, native system software, handset adaptation module, run time engine, basic APIs, and application programs – these are the areas of the core functional specifications of WIPI. Actually, in the WIPI specifications, only the handset adaptation and APIs are included, while the other parts of the functions of the wireless Internet platform are considered as requirements of the handset vendors. The core functions of the WIPI are the handset adaptation and APIs, which are called the HAL and AAL (Application Adaptation Layer), respectively. The HAL defines an abstract specification layer to support hardware platform independence when porting applications; the AAL defines the specifications for the API of the wireless Internet platform, and supports the C/C++ and Java programming languages.

II. ARCHITECTURE OF CELLULAR PHONE BASED RFID

We design a security enhanced RFID middleware to support trust and secure m-business based on RFID [5]. The mobile RFID terminal 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 in figure 2. Here, "Mobile RFID device driver" is the device driver software provided by the reader chip manufacturer.

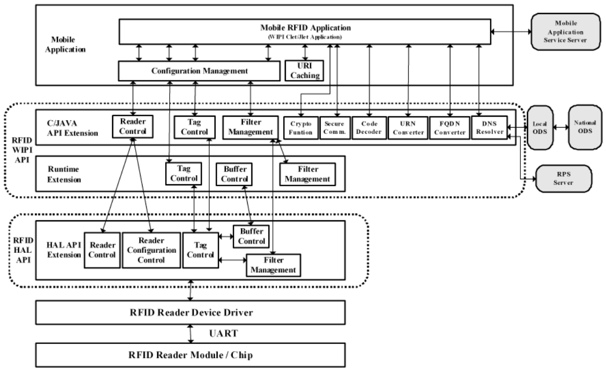

Fig.2. Security Enhanced Mobile RFID Middleware in the Mobile Phone.

This work was supported by the Korea Research Foundation Grant funded by the Korean Government (KRF-2008-357-D00255)

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 IP (Internet Protocol) address of the local ODS server. Figure 3 shows the middleware functions and software. The RFID device handler provides the definitions for the functions of starting the platform and transferring the events from the upper layer of HAL to the RFID H/W Reader. The categories of RFID device handle API cover call, RFID device, network, serial communication, short message service, sound, time, code conversion, file system, input method, font, frame buffer, and virtual key. The AAL provides the definitions for the functions of the adaptive, functions for the RFID engine, WIPI C/Java API, Crypto libraries, and RFID security components.

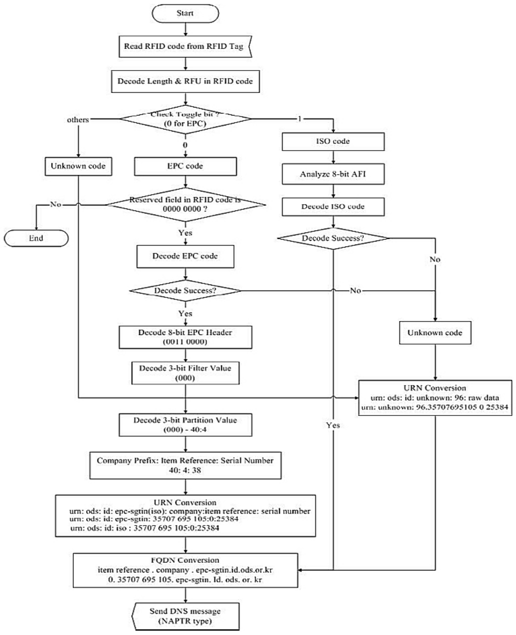
Start
Read RFID code from RFID Tag
Decode Length & RFU in RFID code
Check Toggle bit ? (0 for EPC)
others
1
0
ISO code
Unknown code
EPC code
Analyze 8-bit AFI
Decode ISO code
No
Reserved field in RFID code is 0000 0000 ?
End
Yes
Decode Success?
Decode EPC code
No
Decode Success?
No
Yes
Decode 8-bit EPC Header (0011 0000)
Unknown code
Decode 3-bit Filter Value (000)
URN Conversion
urn: ods: id: unknown: 96: raw data
urn: unknown: 96.35707695105 0 25384
Decode 3-bit Partition Value (000) - 40:4
Yes
Company Prefix: Item Reference: Serial Number
40: 4: 38
URN Conversion
urn: ods: id: epc-sgtin(iso): company:item reference: serial number
urn: ods: id: epc-sgtin: 35707 695 105:0:25384
urn: ods: id: iso : 35707 695 105:0:25384
FQDN Conversion
item reference . company . epc-sgtin.id.ods.or.kr
0. 35707 695 105. epc-sgtin. Id. ods. or. kr
Send DNS message (NAPTR type)

Fig.3. Code Resolution Flow Chart based on Mobile RFID Middleware.

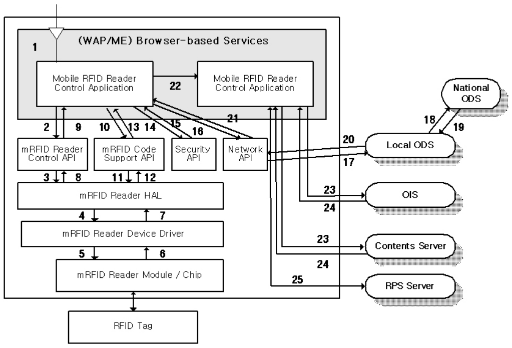

Fig.4. Scenario of Secure Mobile RFID M/W Terminal Function.

Consider a scenario where a mobile RFID client performs an update of its own middleware in the security server, where applying security modules to implement business processes satisfies security requirements. In this scenario, a RFID a service provider which has already been authenticated can perform 1-to-N (from one provider to multiple providers) as well as 1-to-1 business transaction (from one provider to one provider), because it can search and access various RFID middlewares registered in the RFID security server. To offer greater 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.

A secure mobile RFID middleware terminal platform system has been implemented based on the design described in previous section. This is done by applying the proposed mobile RFID middleware terminal platform to system framework and mobile RFID service as shown in figure 5.

Fig.5. Proposed Secure Mobile RFID Middleware's Development.

III. CONCLUSIONS

In this paper we have proposed a mobile RFID architecture which contains several features including security, networking capability, operation scenario, and, code resolution mechanism. The mobile RFID technology is being actively researched and developed throughout the world and more efforts are made for the development of related service technologies. Though legal and institutional systems endeavor to protect privacy and encourage protection technologies for the facilitation of services, the science and engineering world also has to develop proper technologies. In general there it is virtually impossible to have a perfect security / privacy protection system, however, technologies proposed in this paper, would contribute to the development of secure and reliable network RFID circumstances and the promotion of the mobile RFID market.

REFERENCE

[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, pp. 188-193, 2004.

[2] Xiaoyong Su; Chi-Cheng Chu; Prabhu, B.S.; Gadh, R., "Service organization and discovery for facilitating RFID network manageability and usability via WinRFID middleware," *WTS2008,* pp. 392-398, Apr. 2008.

[3] Jongsuk Chae, Sewon Oh, "Information Report on Mobile RFID in Korea," ISO/IEC JTC1/SC31/WG 4 N 0922, *Information paper*, ISO/IEC JTC1 SC31 WG4 SG5, 2005.

[4] S. E. Sarma, S. A. Weis, and D.W. Engels, "RFID systems, security and privacy implications," *Technical Report* MIT-AUTOID-WH-014, AutoID Center, 2002.

[5] 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.* Springer-Berlin, vol. 3842, pp. 741-748, 2006.