

Light-weight RFID Device Interface for Controlling RFID Tag Memory Access

Se Won Oh, Hyochan Bang, Jae Gak Hwang

RFID/USN Research Team, Electronics and Telecommunications Research Institute

161 Gajeong-dong Yuseong-gu, DAEJEON, KOREA

sewonoh@etri.re.kr, bangs@etri.re.kr, jghwang@etri.re.kr

Abstract— This research is about the interface between a RFID reader device and a host for controlling the RFID tag memory access operations. The traditional RFID reader interfaces are often inflexible to deal with the various forms of integration for the heterogeneous RFID reader devices. Also the industries are demanding a RFID device interface to be easier to handle and to improve the processing speed for the RFID tag access operations. Thus, this research analyzes the existing methods for controlling RFID tag memory access, and then proposes a light-weight RFID device interface, called SRP (Simple Reader Protocol). SRP specifies the message formats, supports access operations, and enables the RFID reader configuration about RFID tag memory access. SRP is expected to help the integrated control for the heterogeneous RFID reader devices and further make RFID system development efficient.

Keywords— RFID Reader, RFID Device, Reader Protocol, Reader Interface, Simple Reader Protocol (SRP)

I. INTRODUCTION

Through the radio frequency communication with RFID tags, a RFID reader reads or writes the data which are stored in a RFID tag memory, and also does other memory access tasks including locking/unlocking the data as well as disabling a tag functionality [1]. Figure 1 outlines a RFID system which is composed of a RFID tag, a RFID reader, and a host [2]. Here, a host is an entity which controls a RFID reader device for RFID tag memory access. For example, a host can be either a RFID data monitoring tool, RFID middleware, or a RFID application. The three entities of the RFID system must have two kinds of interfaces for access the RFID tag memory. These are the RFID air interface and the RFID reader interface. First, the RFID air interface is about the communication protocol between a RFID reader device and a RFID tag. As many efforts to standardize the RFID air interface have been made from the international standard organizations as well as from the industrial forums, several specifications have been ratified since 2004, such as ISO/IEC 18000 air interface standards [3] and EPCglobal tag protocol specifications [4]. In particular, ISO/IEC 18000-6 has accommodated the existing requirements for UHF RFID technology and is known as the integrated standard for UHF

RFID air interface. On the other hand, RFID reader interface, or also called as RFID device interface, is about the communication protocol between a RFID reader device and a host. Though there are some specifications ratified as the RFID reader interface, but each one has its own characteristics that might give significant constraints on developing a practical RFID solution.

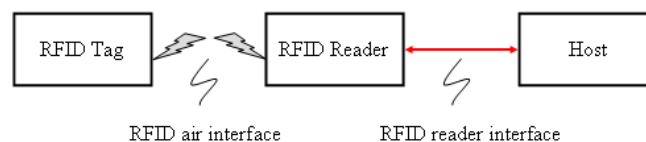


Figure 1. RFID air interface and RFID reader interface

The existing RFID reader interfaces often support only a specific type of RFID reader device product or a specific RFID air interface. As a result, in many cases it is required to pay additional cost to integrate a particular RFID reader device. Furthermore, the existing interfaces are not easy to handle for developing a RFID system because of lots of commands and its complicated base logics. Therefore, the industry became interested in a light-weight interface between a RFID reader and a host, in order to facilitate an efficient access to RFID tag memory [5].

This research proposes the Simple Reader Protocol (shortly as SRP) as the light-weight RFID device interface, which specifies both the command messages and their response messages between a RFID reader device and a host [13]. For example, the basic commands in the SRP include inventory for RFID tags within a RFID reader's reading range, data reading from a RFID tag, data writing to a RFID tag, locking specific data, and killing RFID tag functionality. SRP also considers both the performance for processing large scale of data collected from a RFID reader and the ease of development. In addition, SRP is designed to readily adopt an extended functionality in future as well as custom extension by a specific RFID reader device.

The remainder of this paper is organized as follows: Section 2 introduces the related study. Section 3 proposes the Simple Reader Protocol which specifies message formats and operation types. Section 4 presents a system implementation

which supports SRP, and describes the test cases to make a careful comparison among SRP and the traditional reader protocols. Finally, concluding remarks are provided in Section 5.

II. RELATED STUDY

As a RFID reader interface is usually implemented as a form of software, it is often considered a type of RFID software. And there have been many researches on RFID software as well as the commercialized software products for the last decade ([2], [5]-[7]). Unlike other software technology, however, RFID reader interface is closely related with the standardization to ensure the integrity with the various types of RFID reader devices. So, in this section, the typical usage for the RFID reader interface to develop a RFID solution is described. Then, the existing RFID reader interface protocols are analysed.

A. RFID reader adapter

Most commercial reader manufacturers provide either basic reader interface (BRI) or software development kit (SDK). In many cases, however, these are proprietary and only applicable to their own products or even specific model. So, in order to develop a RFID application system with such a commercial RFID reader device, the host of the system often has to develop a specific adapter module to bring the RFID reader under control. Figure 2 shows a connection structure using a RFID reader module which interfaces both a RFID reader's BRI and a host. If there are three types of RFID reader devices, then three adapter modules has to be developed as shown in Figure 3.

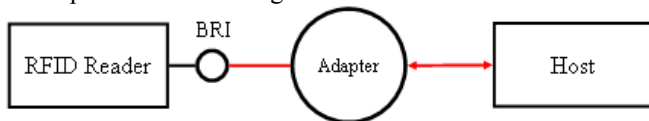


Figure 2. RFID reader adapter

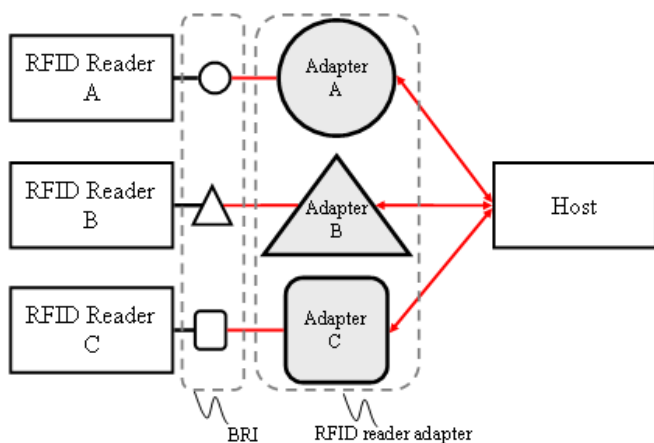


Figure 3. Example of RFID reader interface system structure to support three kinds of RFID reader devices

To solve this adaptability issues, there has been some efforts to make the standard specifications for the RFID reader interface since mid-2000s.

B. RFID reader interface protocols

Table 1 summarizes the existing specifications ratified from several standardization organization including ISO/IEC and EPCglobal. Each specification is not compatible among each other and has its own characteristics as listed in the following tables from Table 2 to Table 6. Since each specification is based on its own complicated processing structure, it has not been easy to use one of them for develop RFID application service for RFID tag memory control.

Table 1. Typical RFID Reader Interface Protocol Specifications

Title	Organization (Year)
ISO/IEC 15961:2004 [8]	ISO/IEC JTC 1/SC 31 (2004)
Reader Protocol v1.1 [9]	EPCglobal (2006)
Reader Management v1.0.1 [10]	EPCglobal (2007)
Low Level Reader Protocol v1.0.1 [11]	EPCglobal (2007)
TTAK.KO-06.0196 [12]	TTA (2008)

ISO/IEC 15961, as shown in Table 2, just provides 16 commands, but each command requires not only the pre-processing tasks including data compaction and formatting, but also understanding many parameters which should be processed according to another specification, ISO/IEC 15962, for data processing. In this case, a host can not process RFID data, if the data is not encoded according to ISO/IEC 15962.

Table 2. RFID Reader Protocol - ISO/IEC 15961

Objective	RFID Tag memory configuration and control
Command Types	16
Message Format	Not specified
Characteristics	- Implementation must be dependent on ISO/IEC 15962 for data encoding

EPCglobal RP specification, as shown in Table 3, requires both a number of logical objects and command parameters just for executing a single tag memory access command, since it is based on a complicated reader object model. For example, to request a RFID reader to read data from a specific RFID tag, the host have to know at least the following reader objects and include them as parameters of the relevant command message. Further each object has to be configured along with other objects such as TagField, ReaderDevice.

- Source
- DataSelector
- TagSelector

Meanwhile, EPCglobal RM specification, as shown in Table 4, can share the same reader object model with EPCglobal RP specification, but focuses on both status monitoring and alarm control of RFID reader device.

Table 3. RFID Reader Protocol - EPCglobal RP

Objective	RFID Reader configuration and abstract reader control
Command Types	148
Message Format	XML, Text
Characteristics	- Based on RFID reader object model - Applicable to only EPCglobal UHF Class 1 Gen1 air interface

Table 4. RFID Reader Protocol - EPCglobal RM

Objective	RFID Reader status monitoring and alarm control
Command Types	93
Message Format	XML, SNMP
Characteristics	- Focuses on controlling RFID reader itself - Applicable to only EPCglobal UHF Class 1 Gen1 air interface

EPCglobal LLRP specification, as shown in Table 5, is less flexible when there are frequent changes in requirements for RFID tag memory access. Specifically, LLRP requires two kinds of scripts such as ROSpec for reader operation and AccessSpec for access operation. And these scripts have to follow the specified state change. Thus, at least four command messages should be sent to the RFID reader from the host in order to execute RFID tag memory access.

- ADD_ROSPEC
- ENABLE_ROSPEC
- ADD_ACCESSSPEC
- ENABLE_ACCESSSPEC

Table 5. RFID Reader Protocol - EPCglobal LLRP

Objective	RFID reader protocol based on air interface characteristics
Command Types	16
Message Format	Binary
Characteristics	- Requires detailed understanding on RF characteristics for setting parameters - Applicable to only EPCglobal UHF Class 1 Gen2 air interface

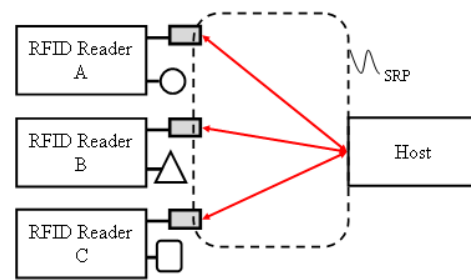
In the other hand, TTA.KO-06.0196, as shown in Table 6, defines RFID reader protocol which is based on mobile phone characteristics, and categorizes command and response sets for both RFID reader configuration and control, as well as for RFID tag memory control.

Table 6. RFID Reader Protocol - TTA.KO-06.0196

Objective	RFID reader protocol for mobile phone
Command Types	38
Message Format	Binary
Characteristics	- Supports a mobile RFID reader - Applicable to only ISO/IEC 18000-6 (Type B, Type C) UHF air interface

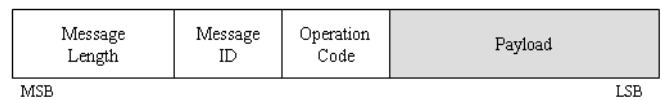
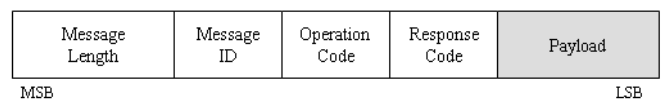
III. SIMPLE READER PROTOCOL

This research proposes a simple reader protocol (SRP) as a light-weight RFID reader interface. The main objective of SRP is to provide a protocol for controlling RFID tag memory accesses. And it aims to make message processing much lighter and faster, and to make adaptable to the general RFID reader devices as shown in Figure 4. In addition, SRP considers the efficiency in implementation and the practical utilization. SRP specifies the message formats between a RFID reader and a host, and also control operations to be executed in a RFID reader.

**Figure 4. Scope of SRP**

A. Message Format

Figure 5 and 6 describes the common message formats for commands and responses, respectively. SRP command message is always sent from the host-side, while SRP response message is always created from the RFID reader-side. Message Length field expresses the length of the message in bytes, and Message ID field is for providing the serial number for each message. And Operation Code field classifies the type of controls which should be executed in a RFID reader.

**Figure 5. SRP command message format****Figure 6. SRP response message format**

B. Operation Codes

Table 7 summarizes the types of control operations and the possible field value which may be expressed in a byte. Among these types, only the five control operations are mandatory to be implemented: Inventory, Read, Write, Kill, and Lock. That is, the other operation code is optional to be implemented. And it should be noted that Notification is a type of response message which is supposed to be periodically created by a RFID reader-side and includes the inventory results during the scheduled period.

Table 7. SRP Operation Types

Category	Description	Operation Code
Inventory	Request the RFID reader to identify the RFID tags which are within its reading range	(0x49, 'I')
Read	Request the RFID reader to read the specific data from the RFID tag memory	(0x52, 'R')
Write	Request the RFID reader to write the specific data to the RFID tag memory	(0x57, 'W')
Kill	Request the RFID reader to disable the functionality of the specific RFID tag	(0x4B, 'K')
Lock	Request the RFID reader to lock or unlock the specific data in the RFID tag memory	(0x4C, 'L')

Get	Retrieve the configuration information from the RFID reader	(0x47, 'G')
Set	Set the configuration information to the RFID reader	(0x53, 'S')
Custom	Custom operation extensible by the RFID reader manufacturers	(0x43, 'C')
Notification	Report from the RFID reader as a result of the periodic inventory operations	(0x4E, 'N')

C. Binary Encoding Format for SRP Messages

SRP messages can be encoded as the following binary encoding format. And the value of a square bracket in each field of SRP message means the byte length to accommodate the field. For example, the value, 2, of the square bracket for Message Length field of Inventory command means that the field should be encoded in two bytes. Since the message length of Inventory command is 5 bytes, the field should be encoded as '0x0005'.

1) Inventory

Inventory command and response message should be encoded as Figure 7. The response message includes N UUI Set parameters as the RFID reader identifies N RFID tags. And the number of RFID tags, N, should be expressed at the Tag Count field. UUI Set parameter structure is specified in Figure 8, and here UUI means the unique item identifier of a RFID tag and UUI header includes the meta-data for UUI. For example, UUI header can be PC (protocol control) bits stored at the UUI memory bank in case of ISO/IEC 18000-6 Type C RFID tag.

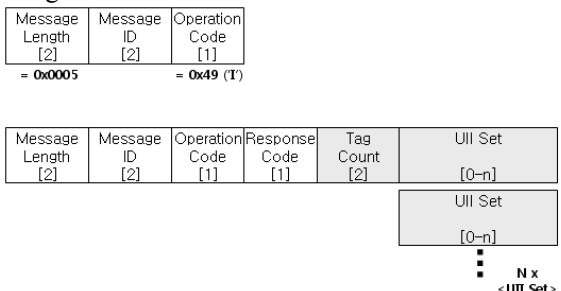


Figure 7. Inventory command and response message

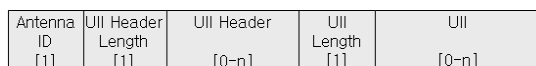


Figure 8. UUI Set parameter

2) Read

Read command and response message should be encoded as Figure 9. This message is to read data stored at the specific memory location of RFID tag which would require passwords to access the data.

3) Write

Write command and response message should be encoded as Figure 10. This message is to write data at the specific memory location of RFID tag which would require passwords to access the data.

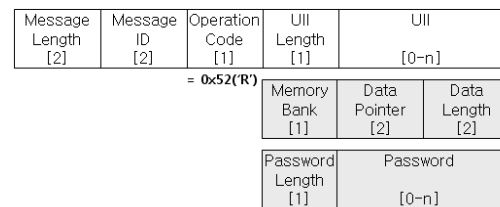


Figure 9. Read command and response message

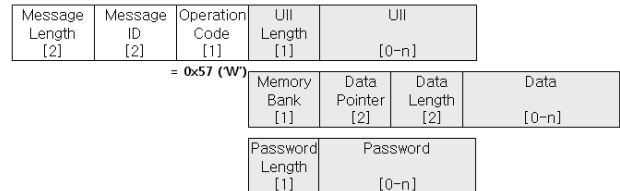


Figure 10. Write command and response message

4) Kill

Kill command and response message should be encoded as Figure 11. This message is to disable the RFID tag functionality. After the successful operation of this command, the specified RFID tag shall not response on any other RFID signal.

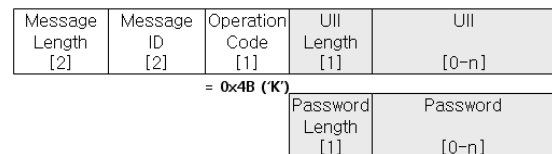


Figure 11. Kill command and response message

5) Lock

Lock command and response message should be encoded as Figure 12. This message is to lock or unlock the specific part of data in a RFID tag which would require passwords to execute this operation.

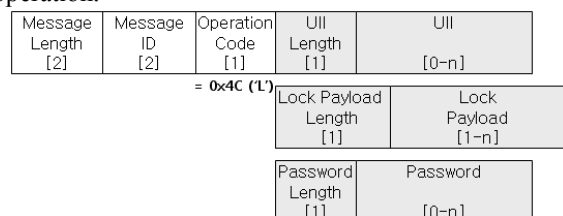


Figure 12. Lock command and response message

6) Notification

Notification message, as shown in Figure 13, is always created from RFID reader. This message includes N AsyncData parameters as the RFID reader identifies N RFID tags. And the number of RFID tags, N, should be expressed at the Tag Count field. Unlike UII Set parameter, AsyncData parameter, as shown in Figure 14, contains the Data field which is for a host to get the specific data along with UII of a specific RFID tag.

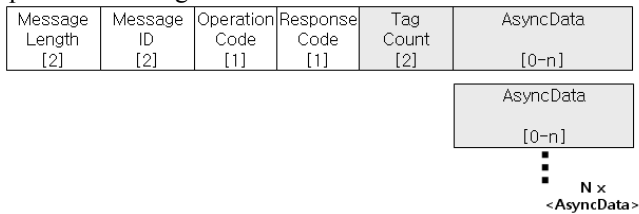


Figure 13. Notification message

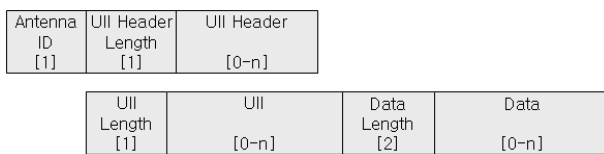


Figure 14. AsyncData parameter

7) Get/Set

Get and Set command and response message should be encoded as Figure 15. The difference between Get and Set command is recognized with the value of Operation Code. This message is either to retrieve the configuration information from the RFID reader or to set configuration with respect to RFID tag memory access.

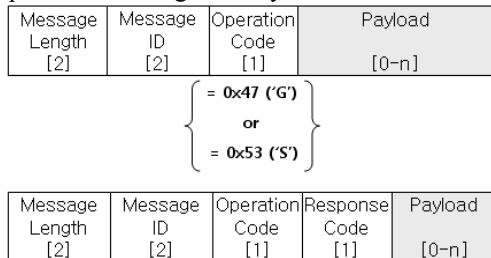


Figure 15. Get/Set command and response message

The payload of both Get and Set message should be encoded as shown in Figure 16. Table 8 summarizes the types of configuration which is implemented to configure the RFID reader device. For example, '0x01' of Config Type field means that the message is about getting or setting the configuration about antenna activation of the RFID reader device.

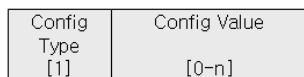


Figure 16. Get/Set message payload

Table 8. RFID Reader Configuration Type

Category	Description	Value
Antenna	Request the RFID reader to	(0x01)

Activation	activate/deactivate the specific set of RFID reader antennas	
Notification Message Activation	Request the RFID reader to activate/deactivate the creation of Notification Messages	(0x02)
Notification Message Setting	Request the RFID reader to set the area to be read from RFID tag memory and to include it in Notification Messages	(0x03)
Tx_Power Control	Request the RFID reader to set the transmit power level	(0x04)
Inventory_Si ze	Request the RFID reader to set the parameter value for inventory operation	(0x05)

IV. SYSTEM IMPLEMENTATION AND TEST CASES

Figure 17 shows a system implementation which interfaces with both a host and a RFID reader device, and which also supports SRP. The numbered procedure describes the steps for a host to connect a RFID reader and then to exchange control messages. In particular, the Device Control Module in Device Interface System creates the SRP command messages for controlling RFID tag memory access operations as well as for setting/getting the configuration related with these access operations. Also, an artifact module for a RFID reader which supports SRP message processing as well as other typical RFID reader interface protocols has been made for the test cases of this section.

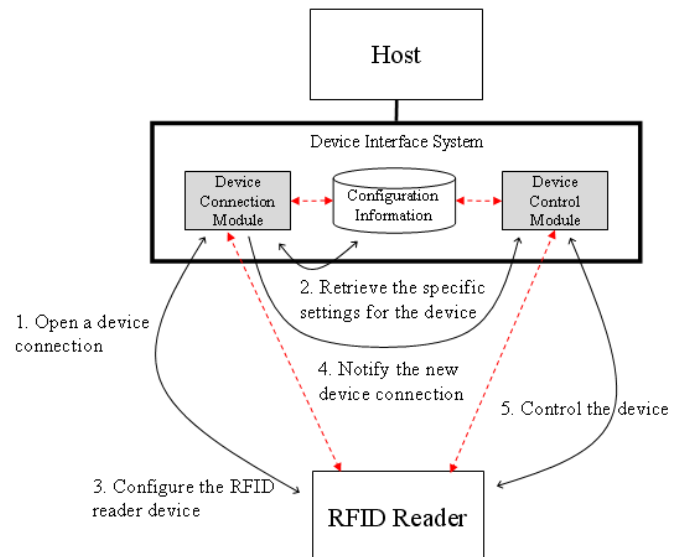


Figure 17. Device Interface System Implementation

Table 9 arranges the test cases that have been experimented on SRP as compared with other typical RFID reader interface protocols. The first 8 cases (F1~F8) is about the functionalities that the specific reader protocol can provide for RFID tag memory access. And their analysis results are shown in Table 10. Table 10 tells that only SRP and LLRP support all the basic functionalities for RFID tag memory access, while the other reader protocols have some limitations.

Table 9. Test Cases

Category	No.	Test Description
Functionality	F1	RFID tags inventory

	F2	RFID tag memory reading
	F3	RFID tag memory writing
	F4	RFID tag killing
	F5	RFID tag locking
	F6	Periodic inventory for the RFID tags
	F7	RFID reader antenna activation
	F8	RFID reader transmit power adjustment
Performance	P1	The time spent for processing 10,000 times of RFID tags inventory commands and responses
	P2	The time spent for processing 10,000 times of RFID tag memory reading commands and responses
	P3	The time spent for processing 10,000 times of RFID reader antenna activation commands and responses
Set-up Steps	S1	The number of commands (or steps) to set-up a RFID reader to read a specific RFID tag memory
	S2	The number of commands (or steps) to set-up a RFID reader to make a periodic inventory report
Adaptability	A1	Adaptation to Passive RFID Air Interface
	A2	Adaptation to Active RFID Air Interface

Table 10. Analysis on Functionalities

Reader Protocol	F1	F2	F3	F4	F5	F6	F7	F8
SRP	O	O	O	O	O	O	O	O
ISO/IEC 15961	O	O	O	X	O	X	X	X
EPCglobal RP	Δ	O	O	O	X	O	O	X
EPCglobal RM	X	X	X	X	X	X	X	X
EPCglobal LLRP	O	O	O	O	O	O	O	O
TTAK.KO-06.0196	O	O	O	O	O	O	X	O

The other results regarding performance, set-up steps, and adaptability are arranged in Table 11. Regarding the test cases about performance, EPCglobal RM do not support all these test cases, while EPCglobal LLRP do not provide any direct command message for these test cases. Likewise ISO/IEC 15961 and EPCglobal RP don't have available commands for some of these tests. In addition, tests with TTAK.KO-06.0196 are excluded, since it is just for the RFID reader module embedded in the mobile phone terminal. The test results from P1, P2, and P3 are marked in 'seconds' that have been spent to execute each test. Relatively, the result from SRP shows good when compared with the other test groups because of its small message packet size.

Table 11. Analysis on Set-up and Adaptability

Reader Protocol	P1	P2	P3	S1	S2	A1	A2
SRP	24	22	69	1	2	O	O
ISO/IEC 15961	60	142	X	1	X	O	O
EPCglobal RP	-	125	-	3~	12	O	X
EPCglobal RM	X	X	X	X	X	O	X
EPCglobal LLRP	-	-	-	4~	4~	O	X
TTAK.KO-06.0196	-	-	-	1	2	O	X

In case of S1, SRP, ISO/IEC 15961, TTAK.KO-06.0196 requires only one step of command to satisfy the goal, while RP and LLRP requires at least 3 or 4 steps of message exchanges between a host and a RFID reader.

In case of S2, SRP and TTAK.KO-06.0196 requires the fewest steps, LLRP requires at least 4 steps for generating automatic inventory results. And RP even requires 12 steps as the follow series of command message exchange;

- Trigger_create
- Source_create, _addReadPoints
- Source_setReadCyclesPerTrigger, _addReadTriggers
- DataSelector_create, _addFieldNames
- DataSelector_addEventFilters
- NotificationChannel_create, _setDataSelector
- NotificationChannel_addNotificationTriggers
- NotificationChannel_addSources

Meanwhile, TTAK.KO-06.0196 only gets UII inventory result from S2, while SRP enables for a host to get other RFID data along with UII inventory result.

Regarding the test cases about adaptability, only SRP and ISO/IEC 15961 don't have limitation on the air interface that the RFID reader is based on.

V. CONCLUSIONS

The proposed interface, SRP, is expected to improve efficiency for integrating RFID reader devices, and to minimize any confusion in utilizing RFID technology for application service development. Recently, SRP has been adopted as an industrial standard specification in December 2009. As many RFID applications based on SRP appears in future, SRP will contribute to develop ubiquitous infrastructures and to solve other RFID challenges, by providing heterogeneous RFID reader control in ubiquitous network environment.

ACKNOWLEDGMENT

This work was supported by the Ministry of Knowledge Economy (MKE) of the Republic of Korea. [2006-S-022-04, Development of RFID/USN Middleware Platform Technology]

REFERENCES

- [1] K Finkenzeller, *RFID handbook: fundamentals and applications in contactless smart cards and identification*, 2nd ed., R. Waddington, Ed. West Sussex, England: John Wiley & Sons Ltd, 2003.
- [2] Q. Z. Sheng, X. Li, and S. Zeadally, "Enabling next-generation RFID applications: Solutions and challenges," *Computer*, vol. 41, pp. 21–28, Sept. 2008.
- [3] (2009) The ISO website. [Online]. Available: <http://www.iso.org/>
- [4] (2009) The EPCglobal website. [Online]. Available: <http://www.epcglobalinc.org/>
- [5] Y. Ouyang, J. Hao, T. Zhang, Q. Ren, and Z. Xiong, "Research on lightweight RFID Reader Protocol," in *Proc. Ubi-Media Computing*, 2008, p. 32.
- [6] S. Oh, Y. Kim, and Y. Lee, "RFID-based Middleware System for Providing Ubiquitous Information Service," *IPSI SIG Technical Reports*, vol. 2005, pp. 461–466, 2005.
- [7] C. Floerkemeier and M. Lampe, "RFID middleware design: addressing application requirements and RFID constraints," in *Proc. Joint sOc-EUSAI conference*, 2005, p. 219.
- [8] *Information technology -- Radio frequency identification (RFID) for item management -- Data protocol: application interface*, ISO/IEC 15961, 2004
- [9] *Reader Protocol (RP) Standard v1.1*, EPCglobal, 2006
- [10] *Reader Management (RM) Standard v1.0.1*, EPCglobal RM, 2007
- [11] *Low Level Reader Protocol (LLRP) Standard v1.0.1*, - EPCglobal, 2007
- [12] *Mobile RFID Reader Control Protocol*, TTAK.KO-06.0196, TTA, 2008
- [13] *Simple RFID Reader Protocol for Controlling RFID Tag Memory*, TTAK.KO-06.0220, TTA, 2009