Mobile RFID Applications and Security Challenges

Konidala M. Divyan, Kwangjo Kim

Information and Communications University (ICU),
International Research Center for Information Security (IRIS)
R504, 103-6, MunjiDong, Daejeon 305732, Republic of Korea
{divyan, kkj}@icu.ac.kr

Abstract. With mobile RFID technology, handheld portable devices like mobile phones and PDAs, also behave as RFID readers and RFID tags. As RFID readers, mobile phones provide an user-friendly approach to quickly and efficiently scan, access and view information about RFID tagged items. As RFID tags, mobile phones can quickly identify themselves in order to communicate with other tagged devices, which provide essential services. At the outset this paper briefly describes Mobile RFID technology and compare it with conventional RFID technology. We pioneer in categorizing Mobile RFID applications into three distinct zones, namely: Location-based Services (LBS) Zone, Enterprise Zone, and Private Zone. We describe application scenarios related to these zones and highlight various security and privacy threats. Finally, we propose a security architecture for LBS zone and describe our future work.

1 Introduction

1.1 RFID Technology

Radio Frequency Identification (RFID) [1] is a means to efficiently and quickly, auto-identify objects, assets, pets, and people. So far, few big companies like Wal-Mart, Proctor & Gamble Co., and Gillette *etc.*, are using RFID technology for real-time tracking of inventory in their supply chain. With the current bar-code technology, each product's bar-code label must be brought before the reader, and labels must be scanned one by one. This leads to laborious, human-error prone, and time consuming inventory check, and also causes customers in a store to wait in long queues at the cashier counter.

Whereas with RFID technology, passive RFID tags are attached to objects/products and these tags contain tiny, but durable computer chips with very small antennas. Passive tags are powered-up from the interrogation Radio-Frequency (RF) signal of a reader. The tiny computer chips contain an Electronic Product Code (EPC) that uniquely identifies the object to which it is attached to, and the antennas automatically transmit this EPC number without requiring line-of-sight scanning, to RFID readers within a certain RF range. The unique EPC number is like a pointer directing the RFID reader to the right Information Server on the EPC Network from where the reader can download additional

related data about the product it scanned. Therefore RIFD technology allows quick scanning of products in large bulks (*e.g.,* a whole pallet at a time) thus speeding up the supply chain management

Other advantages of RFID technology include: RFID tags can stand a harsh environment, long read ranges, portable database, multiple tag read/write, and tracking items in real-time, *etc.* [5] gives a good description about RFID technology for supply chain management. RFID automates supply chain management, enabling enterprises to realize significant savings to the top and bottom line. RFID technology greatly helps enterprises to maintain the accuracy of shipments sent and received by parties throughout distribution. As a result we can keep a check on product theft, product counterfeiting, and it also helps in precise product recall.

1.2 Mobile RFID Technology

Currently RFID tags are still expensive, but very soon it would become economical to tag products at the item level. This will open the door for large-scale use of RFID tags on consumer goods. As a result, in near future we can realize, one of the visions of automatic identification and ubiquitous computing, which is the creation of an "Internet of Objects". In such a highly connected network; devices, objects, items of any kind dispersed through an enterprise or in our society can talk to each other, providing real-time information about the objects, location, contents, destination, and ambient conditions. This communication allows much-sought-after, efficient and easy machine-to-machine identification, communication, and decision-making [1]. Thus RFID technology will have a tremendous impact on our society, once it starts to assist people in their daily lives. A right step in this direction is Mobile RFID technology.

With mobile RFID technology, handheld portable devices like mobile phones and PDAs, apart from having the usual voice/data communicating features, also behave as RFID readers and RFID tags. As a result, Mobile RFID brings the conventional RFID technology closer to common users rather than just constraining it's usage to supply chain management. The following section describes the various applications of Mobile RFID technology.

1.3 Applications of Mobile RFID Technology

With Mobile RFID technology users can efficiently perform two major tasks, namely: download and view information represented by RFID tags, and machine-to-machine identification and communication.

Download & View Information represented by RFID tags: Just by bringing a Mobile RFID enabled portable device near to a RFID tagged object, we can quickly and easily download information represented by that RFID tag and view that information via mobile device's display screen. For example:

– We can download information about a particular location by scanning RFID tagged sign posts, and landmarks.
– We can download bus routes by scanning RFID tagged Buses.
– We can download prices of RFID tagged merchandise sold at stores, and published in catalogs for Smart Shopping.
– We can download movies, music, trailers, show timings, and theater locations by scanning RFID tagged movie posters, music CDs, *etc.*

Machine-to-Machine identification and communication: When Mobile RFID enabled portable device behaves as a RFID tag we can consider the following applications:

– We can authenticate ourselves to a RFID reader in order to access a particular facility (building, home, *etc.*) or services.
– We can carryout micro payments at subway stations, bus, newspaper stands, and gas stations by bringing our mobile device near to a RFID reader.
– We can give out information about our mobile device's model no. and size of it's display screen, in-order to download and view suitable multimedia content from a multimedia kiosk.
– We can make a quick call or send an instant message by scanning RFID tagged photographs, business cards, address books, *etc.*

We strongly believe that Mobile RFID technology has a great future and it's a very challenging research area. It is poised to be one of the future killer applications and services for mobile communications field.

1.4 Mobile RFID Application Zones

Mobile RFID applications can be broadly categorized into three zones namely: Location-based Services (LBS) Zone, Enterprise Zone, and Private Zone. From now on and Henceforth we consider a "mobile phone" to be our portable device, which has Mobile RFID enabled technology, *i.e.,* this mobile phone is incorporated with both RFID reader and tag functionalities. In the subsequent sections we describe each of these zones and their corresponding security and privacy threats.

2 Location-based Services (LBS) Zone

In a LBS zone, service providers provide services that are "related to" and "available at" customer's current location. The coverage of this zone is very large, which includes all public places, roads, shopping malls, cinema halls, and food courts, *etc.* Service providers deploy RFID tagged items/devices (*e.g.,* posters, sign boards, maps, shopping catalogs, commodities, digital photo printers, multimedia servers, and RFID readers to receive payments, *etc.*) all around, which will enable us to carry out the above-mentioned two major tasks.

2.1 Security for Mobile RFID at LBS Zone

In this section we describe various security threats related to Mobile RFID at LBS Zone and later propose a security framework. Table 1, summarizes the security assessment of this zone.

In LBS zone, most of the RFID tags respond to every mobile phone, otherwise the main purpose of these tags to provide "location-based instant information" would be defeated. Therefore, we do not consider a tag-reader mutual authentication and strong secure communication between RFID tag and mobile phone. But there is one problem, these publicly available tags can be fake or must have been illegally modified (cloned) and no longer truly represent the information of the item in question. As a result, we at least need a one-way authentication mechanism, which authenticates the RFID tag to the mobile phone. [2] provides description of some of the RFID tag-reader authentication schemes that better serve this purpose. The most popular among them are challenge-response schemes that are based on symmetric key encryptions, hash functions, and hash chains.

Also we assume that for this task in LBS zone, most of the items/products are tagged with low-cost passive RFID tags like EPCglobal Class-1 Generation-2 UHF tags [4]. Generally a user's mobile phone may be used to scan one RFID tag at a time, we assume that the distance between the RFID tag and the mobile phone is too short to consider an active eavesdropping by an adversary. For further security assessment, let us consider the following scenario:

Scenario: *Alice visits a shopping mall. She uses her mobile phone to scan RFID tags attached to various items that are being sold. After scanning a particular RFID tag, the mobile phone is allowed to access shopping mall's "Information Server (IS)", which contains a detailed database about the scanned RFID tag. As a result, the mobile phone can download and store the price, picture, features, and manufacturer details of that item. The mobile phone must not be allowed to download other sensitive details like the number of pieces sold so far, its profit margin, and stock availability,* etc., *in order to prevent corporate espionage, this information is strictly for the shopping mall's inventory checking staff. Alice's mobile phone must also be protected from being directed to, accessing, downloading information, from malicious IS. Malicious IS can either induce virus code into to the mobile phone or extract sensitive data off the mobile phone. Alice must be able to scan tags in the shopping mall anonymously without revealing her true identity and buying habits. The shopping mall must be able to verify Alice's age incase she wants to download details about alcohol, and mature books or multi-media content. On the other hand, Charlie, an adversary, stalks Alice into an elevator. Charlie must be prevented from using his mobile phone to scan and retrieve sensitive information off any RFID tagged item that Alice is carrying in her bag/purse.*

From the above scenario, we identified the following security threats and security requirements:

Secure Job Delegation & Trust Model: There would be many competitive service providers selling location-based services to users. A user's mobile phone may need to communicate with many service provider's Information Server. Mobile phone should identify and authenticate genuine information servers and be able to secure the entire transaction and also protect the owner's privacy. But these tasks could create a huge burden on the low-computing and resource-poor mobile phone and is certainly not user friendly. Therefore it would be lot easier for the mobile phone to securely delegate its work to a trusted high-computing and resource-rich entity, such as a mobile operator. This approach helps in reducing the communication and computational burden on the mobile phone. Establishing an efficient and a convincing trust model is very much required to ensure secure transactions, key distribution, and job delegation. With existence of a trust model, it would be lot easier for the mobile phone to delegate its work to the mobile operator.

Detect Malicious Tag Information Servers User's mobile phone must be allowed to access and download information from only genuine and authentic tag information servers. Therefore it is essential to authenticate and authorize every information server that the mobile phone is trying to access.

Authorized Tag Information Access: Some of the information represented by RFID tags must be available to only authorized people. But with the onset of Mobile RFID technology, RFID readers (incorporated into mobile phones) will soon become ubiquitous. Therefore it becomes essential for information servers to categorize which user's mobile phone is entitled to download what kind of information. This requires efficient authentication, authorization, and access-control protocol. Information represented by RFID tags must be made available to mobile phones, based on the privileges of the user *e.g.,* customer, staff, juvenile, adult, gold/platinum member of an organization, *etc.*

User Privacy Protection: After scanning a particular RFID tag for information, the identity and location of user must not be revealed to the service provider. This personal information could allow service providers and vendors to generate detailed profiles of the user, his buying interests, and transactions information. Adversaries must not be able to scan RFID tagged items already purchased by users.

Data Integrity & Confidentiality: We require secure Electronic Data Interchange (EDI) between the mobile phone and service provider's Information Servers.

Table 1 gives the summary of security threats and security requirements for this zone. We consider two distinct communication channels between: Mobile Phone & RFID Tag (for scanning a tag), and Mobile Phone & Service Provider's Information Server (for retrieving information represented by the tag).

Threat	Security Req.	Tag ↔ MP	MP ↔ SP-IS
User ID Privacy	Pseudonyms	O	O
	Anonymous Credential	O	O
Illegal Info. Access	Authentication	O	O
	Authorization	X	O
	Access Control List	X	O
Eavesdropping	Encryption/Decryption	X	O
	Digital Certificate	X	O
Key/Pwd Compromise	Trust Model	X	O
	Key/Pwd Management	X	O
MP: Mobile Phone	SP-IS: Service Provider's IS	X: Not Req.	O: Req.

Table 1. Mobile RFID-LBS Zone Security Assessment

3 Building Blocks: Mobile RFID - LBS Zone

The building blocks of Mobile RFID infrastructure in LBS zone is similar to EPCglobal's RFID infrastructure. EPCglobal [6] is leading the development of industry-driven standards for the Electronic Product Code (EPC) to support the use of Radio Frequency Identification (RFID) in supply chain management. Due to space constraint we do not explain the EPCglobal RFID System Architecture. But the details we provide can be understood easily. Expect that we introduced mobile operator and eliminated the need of EPC Middleware. Since mobile RFID would mostly scan one tagged item at a time, there is no need for filtering software to make the mobile RFID data clear.

- Mobile RFID (M-RFID): Mobile Phone with both RFID Reader and Tag functionalities, is used to scan tagged items available everywhere.
- RFID Tags: every RFID tag contains its unique EPC number. EPC is a globally unique serial number that identifies an item in the supply chain. EPC data/number contains: EPC Manager number (identifies the company), Object class (similar to a stock-keeping unit, also called product number), Serial number (specific instance of the object class being tagged, objects own unique identifier). EPCglobal allocates manufacturers specific blocks of EPC numbers, and manufacturers then add their own product codes and serial numbers to their assigned manufacturer numbers to create unique identifiers - EPCs.
  Further information about the product is stored on a network of servers and databases called EPC Network. Therefore, unique EPC number acts like a pointer directing the RFID reader to the right entity on the EPC Network from where the reader can download additional related data about the product it scanned.
- Mobile Operator (MO): In the current mobile communications paradigm we have already put in a great deal of trust in MO, as it handles all our

voice and data communications. It maintains a record of each subscriber's call details, contact information, and credit card details, *etc.* It even has the capability to easily determine our current location and tap into our communications. But what protects us from MO turning hostile is that it has to very strictly adhere to and follow legal, security and privacy policies imposed by the law. Our architecture extends this trust in MO to secure and provide privacy protection for Mobile RFID transactions. This approach is very practical and easily deployable, as the current mobile communications infrastructure is widely spread and highly stable. MO takes responsibility on behalf of M-RFID to select, identify, and authenticate genuine ECP-IS. MO behaving like a "Trusted Proxy" processes the request on behalf of the M-RFID, greatly reducing the communication and computational burden on the user's mobile phone and also provides users privacy protection. MO also takes responsibility on behalf of M-RFID to select, identify, and authenticate only the genuine SPs and their information servers.

– EPC Network: Just like the global look-up system such as the Domain Name Service (DNS), VeriSign [5], after obtaining the contract from EPCglobal, has invested heavily in building and marketing an EPC Network specifically to look up EPC data. It becomes very necessary to look up each EPC number on a central data repository like we do with a Web page or other system using DNS. Keeping EPC data as an unique reference or primary ID, further information about the respective product is stored on databases and servers of EPC Network. This network assists local company staff and geographically distributed supply chain partners to easily and efficiently access information on any product they are handling from any location. The EPC Network [5] consists of three main components: Object Naming Service (ONS), the EPC-Information Services (EPC-IS), and the EPC-Discovery Services (EPC-DS).

4 Security Architecture: Mobile RFID - LBS Zone

This section describes our proposed security architecture of the Mobile RFID as depicted in Figure 1.

– Step 1: M-RFID scans a RFID tag
– Step 2: RFID tag responds with EPC number
– Step 3: M-RFID authenticates itself to MO via login ID/pwd and sends the EPC number to MO
– Step 4: MO sends EPC number to the ONS
– Step 5: ONS responds with URL of the EPC-IS related to the EPC number in question
– Step 6: MO fetches the anonymous M-RFID certificate from its database and sends it along with EPC number to the URL of EPC-IS. The certificate does not contain the identity of M-RFID but contains some related information like age, proof of privileged membership, *etc.*
– Step 7: EPC-IS verifies the certificate and checks the access-control list in its database.

– Step 8: Depending on the access rights of that certificate, EPC-IS responds to MO with related data about the EPC number in question.
– Step 9: MO sends the EPC information to the M-RFID. This communications can be encrypted using an established session-key
– Step 10: MO stores details of this transaction in the database of this M-RFID. Later, M-RFID can query some information about the tags it accessed previously on a particular date, time, location (for compare shopping) and also items it purchased.
– Step 11: M-RFID can purchase tagged items. MO can pay the vendor on behalf of M-RFID and later get the money from M-RFID via monthly telephone bills.

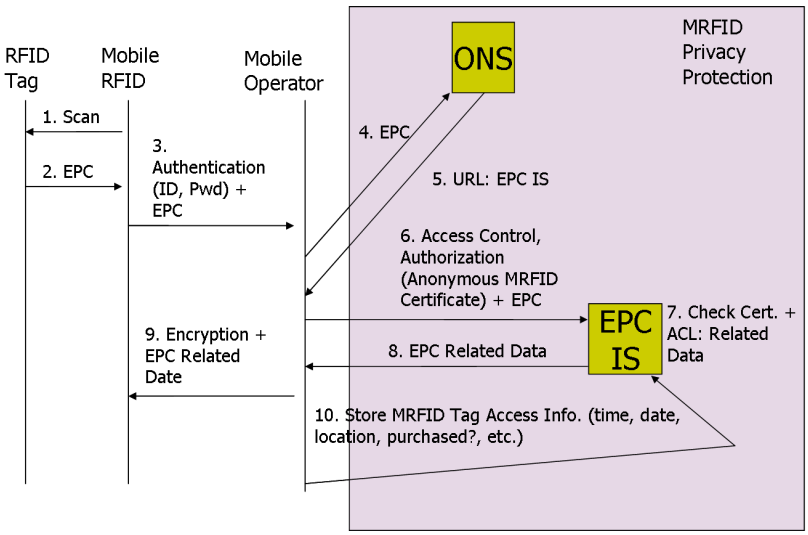

Fig. 1. Mobile RFID - LBS Zone Security Architecture

4.1 Security Solutions

Mutual Authentication mechanism between M-RFID and MO A simple ID/Password authentication for M-RFID and MO's PKI certificate verification by M-RIFD is necessary for mutual authentication between M-RFID and MO. This provides secure job delegation, trust model, data integrity and confidentiality between M-RFID and MO.

Mutual Authentication mechanism between MO and EPC-IS MO takes responsibility on behalf of M-RFID to select, identify, and authenticate only the

genuine SPs and their information servers. This protects M-RFID from accessing malicious EPC-IS servers. Since MO and EPC-IS are resource rich entities, they both can authenticate each other via PKI-based certificates. Thus providing data integrity and confidentiality.

Anonymous Certificates for Identity management, authentication, and authorization M-RFID can request anonymous certificate from MO. This certificate does not contain the true identity of M-RFID but contains other details like age, whether the user is a gold card member or not, staff or visitor, *etc.* This protects the privacy of the owner of M-RFID and also assists EPC-IS to provide corresponding information about the EPC number in question.

M-RFID privacy Our approach protects both location and information privacy of M-RFID. With the use of anonymous certificate the vendor or the service providor of the tagged item can never know the true identity of the M-RFID's owner. To prevent an adversary from scanning the handbag of Alice, and obtain information about the tagged items purchased by her, we suggest the following two approaches:

Kill the Tag: EPCglobal Class 1 Gen 2 UHF Tags [4] can be embedded with Kill Password. Whenever a RFID reader send this Kill Password to the tag, the tag is killed and rendered permanently unusable and unreadable. Therefore, once a tagged item is purchased by M-RFID, the trustable clerk at the point of sale (cash counter) can obtain the tag's kill password from the shopping mall's information server and using this kill password the clerk can kill the tag permanently. But this approach has a drawback if the customer wants to make use of the tag capabilities at his home, *e.g.,* RFID enabled refrigerator or book shelf, *etc.*

Lock the Tag: EPCglobal Class 1 Gen 2 UHF Tags [4] can be embedded with a 32-bit value Access Password, which means that only a reader that already possesses the right access password can perform mandatory commands on the tag, such as Read, Write, and Lock. Therefore tag's access password can be used for "reader to tag" authentication and in the process allows the reader to access the locked memory banks within the tag, permission to change the lock status of the memory banks, and write data into the tag, etc. A tag has four memory banks: Reserved, EPC, TID, and User. Reserved memory bank is used to store the Kill Password and Access Password, EPC memory bank for EPC number, TID memory bank for tag's unique manufacturer identity number, and User memory bank for additional user data. The reserved memory bank of the tag is permanently locked; as a result the access password can neither be read nor modified by any reader.
Therefore once a tagged item is purchased by M-RFID, the trustable clerk at the point-of-sale (cash counter) can obtain the tag's access password from the shopping mall's information server and using this access password the clerk can lock all the memory banks of the tag including the EPC memory

bank. The M-RFID can obtain and store the tag's access password at the point-of-sale. Now the customer can use his/her M-RFID to lock and unlock the tag whenever and wherever required. Since an adversary does not know the tag's access password he can no longer track or get any data from the tag as all the memory banks are locked. Through this approach the tag need not be killed permanently.

5 Enterprise Zone

In this zone mobile phone assists company's mobile staff/employees like inventory checkers, field engineers, maintenance and repair staff, and security guards. It helps them in real-time inventory management, work attendance log, instructions on how to operate tagged items, 'identification of' and 'access control to' tagged equipment and secure enclosures, and proof of staff presence at certain locations in a building that needs to be monitored periodically, *etc.*

The security framework for enterprise zone Mobile RFID applications could be proprietary and confined to the boundaries of a particular organization. In such a confined and well-monitored zone it's not very difficult to establish and enforce an efficient security architecture, trust model, and security & privacy policies. With the availability of up-to-date list of registered employees and items/products in a company; designing and implementing key/ password distribution, data integrity & confidentiality, identification, authentication, and access control protocols among staff, RFID readers, RFID tagged items, and EPC Network is moderately easy and mostly risk free when compared to LBS zone.

Since this zone needs precise authentication and security auditing in order to access RFID tagged items, we require tag-reader mutual authentication and also the true identity of the M-RFID must be revealed, therefore user privacy may not be needed. Table 2, summarizes the security assessment of this zone.

Threat	Security Req.	Tag ↔ MP	MP ↔ E-EPC
User ID Privacy	Pseudonyms	X	X
	Anonymous Credential	X	X
Illegal Info. Access	Authentication	O	O
	Authorization	O	O
	Access Control List	X	O
Eavesdropping	Encryption/Decryption	X	O
	Digital Certificate	X	O
Key/Pwd Compromise	Trust Model	X	X
	Key/Pwd Management	O	O
MP: Mobile Phone	E-EPC: Enterprise's EPC n/w	X: Not Req.	O: Req.

Table 2. Mobile RFID-Enterprise Zone Security Assessment

5.1 Private Zone

In this zone, mobile phone assists users in their private space like home, garden, garage, car, and workshop. It helps them to make an instant call or send an instant message by scanning RFID tagged photographs, business cards, and address books. By scanning RFID tagged household items with a mobile phone, we can quickly obtain information like; when would the milk stored in the refrigerator expire, details of the books in the bookshelf, when was the last time a RFID tagged plant has been watered, and when to change the engine oil, *etc.*

This zone is small when compared to the other two zones and therefore it requires a simple security model that can be easily deployed and maintained by the user at his home. Users in this zone can buy off-the-shelf Mobile RFID Kits. These kits can contain RFID tags, Mobile RFID, related hardware, and software with user-friendly GUI. The software can assist the users to easily encode EPC numbers of their choice into the RFID tags, create a portable database in their PC with details about the tagged household items, create passwords to access these tags and the database, and finally secure the wireless/WiFi network in the home environment.

Other option could be, the user can obtain storage space (for free or fee) on the EPC Network (EPC-Information Servers) and via a password protected user-friendly website, he can upload his personal EPC numbers and details of the tagged household items. Whenever he scans his private RFID tag in his home, the Mobile RFID contacts his personal page on the EPC-Information Server and downloads the details about the item in question. This approach alleviates user's burden of configuring his own security system. The EPC-Information Server must provide user privacy protection, and secure communication.

We need to protect this zone from malicious RFID readers sitting outside this zone and trying to track the RFID items inside the zone (*e.g.,* all the expensive items inside the home that are worthwhile to steal). To ward off this threat we need reader to tag authentication. The tag must allow only authorized readers from within the home to scan and query it. Other approach is to install equipment outside the home, that would jam any external malicious noise or radio signals from entering inside the home. Sometimes it may be required that the children, guests and visitors to this zone are provided with different access control rights to the tagged devices. Therefore we need user identity and access control list, which specifies the rights and capabilities of the users in this zone. Table 3, summarizes the security assessment of this zone.

6 Conclusions

This paper provides future vision and security challenges of Mobile RFID. We mentioned the various security threats and security requirements at different zones of Mobile RFID applications namely LBS, enterprise, and private zones. And proposed a simple security architecture for the LBS zone, that fits the RFID EPC Network. The advantages of this architecture are as follows: simple,

Threat	Security Req.	Tag ↔ MP	MP ↔ U-EPC
User ID Privacy	Pseudonyms	X	X
	Anonymous Credential	X	X
Illegal Info. Access	Authentication	O	O
	Authorization	O	O
	Access Control List	X	O
Eavesdropping	Encryption/Decryption	X	O
	Digital Certificate	X	O
Key/Pwd Compromise	Trust Model	O	O
	Key/Pwd Management	O	O
MP: Mobile Phone	U-EPC: User's Private EPC n/w	X: Not Req.	O: Req.

Table 3. Mobile RFID-Private Zone Security Assessment

involves less user interactions, secure job delegation between Mobile RFID and Mobile Operator. Also the Mobile Operator conceals the identity of users, as a result service providers and vendors of tagged items cannot maintain users detailed profiles and location information, this protects users privacy. It could be a good revenue generator for the mobile operator and service providers through commissions for every transaction. Our approach is practical and easily deployable, as the current mobile communications infrastructure is widely spread and highly stable. And vendors can still use the the popular RFID EPC network. As our future work we would propose more concrete security architectures for the other two zones of Mobile RFID applications and also propose a simple, secure and privacy preserving payment phase for Mobile RFID applications.

Acknowledgement: This work was supported in part by "Development of Sensor tag and Sensor node technology for RFID/USN" project of ETRI through IT Leading R&D Support Programs of MIC, Korea

References

1. Patrick J. Sweeney II, "RFID for Dummies", Wiley Publishing,Inc., ISBN: 0-7645-7910-X, 2005.
2. Ari Juels, "RFID Security and Privacy: A Research Survey", RSA Laboratories, 2005,
3. EPCglobal Web site, 2005, `http://www.EPCglobalinc.org`
4. EPCglobal Inc., "Class 1 generation 2 UHF air interface protocol standard version 1.0.9.", Referenced 2005 at `http://www.epcglobalinc.org/standards/`
5. VeriSign, "The EPCglobal Network: Enhancing the Supply Chain", White Paper 2005, `http://www.verisign.com/stellent/groups/public/documents/white_paper/002109.pdf`
6. EPCglobal Specification, "EPCglobal Architecture Framework Version 1.0", `http://www.epcglobalinc.org/standards/`