STANDARDS, SECURITY & PRIVACY ISSUES ABOUT RADIO FEQUENCY IDENTIFICATION (RFID)

Evsen Korkmaz[1], Alp Ustundag[2] and Mehmet Tanyas[3]

Abstract

There is no doubt that managing the flow of goods depends on monitoring the real flow in the physical world meanwhile in the digital world. Today automatic identification (auto-ID) technologies are used to close the gap between these two different environments by online updating of databases as the materials flow in the chain. From this point of view, we can say that auto-ID technologies are core components of automated inventory control systems on all echelons of supply chain. As being a novel sub-component of auto-ID, RFID innovates important features. Although developments in RFID technology begun nearly 50 years ago, recent advances provided new opportunities improving commerce and everyday life. New applications and obligations (like the obligations that are put forward by Wal-Mart to its suppliers) bring forth different aspects. Due to the fact that RFID is a recently developed technology, there exist some deficiencies, like the lack of standardization and the lack of legislation regulations, that cause questions about privacy and security in society. In this study, we reviewed the standardization studies of related organizations like EPCglobal and ISO, compare these and find the gaps. We also classify the risks that threaten the privacy of individuals and organizations. Finally, regarding the standardization studies and existing risks towards the privacy of individuals and organizations, security proposals and policy suggestions are introduced.

Keywords: *Automatic Identification (auto-ID), Radio Frequency Identification (RFID), Security, Privacy, Standardization, Supply Chain Management (SCM)*

1. Introduction

RFID (Radio Frequency Identification) technology is the latest Auto-ID technology that is anticipated to supersede the barcode technology. As its name implies, RFID uses radio signals to communicate. There are three main components of RFID systems. These are tag, reader and back-end database (Weis, 2003). The communication between these components is provided by radio waves like the other wireless technologies as Bluetooth. RFID represents several distinctions over barcodes in terms of (1) non optical proximity communication, (2) information density, (3) two way communication ability and (4) multiple simultaneous reading (read more than one item at once) (Roberts, 2006). These features provide RFID the advantage of expanding all echelons of the supply chain. While the manufacturing of RFID tag technology is evolving, it is planned to develop tiny tags that are invisible to the human eye. The microscopic beads (RFID tags) can be embedded in inks to track banknotes and other important documents. The microscopic tags can also be added to the materials like automobile paint, explosives, or other products that law enforcement officers or retailers have a strong interest in tracking. According to researchers, this technology could be ready for commercial use in three to six years (http://epic.org/privacy/rfid). The other constraint that lays in the future proliferation of RFID tags is cost of tags. A barcode label can be produced at a cost of less than 1 cent per label. So the main drawback of RFID against the barcode is cost of tags. According to the RFID tag classes, the cost also differentiates. Whereas

[1] Istanbul Technical University, Turkey, +90 212 293 13 00 , korkmazev@itu.edu.tr
[2] Istanbul Technical University, Turkey, +90 212 293 13 00-2759 , ustundaga@itu.edu.tr
[3] Istanbul Technical University, Turkey, +90 212 293 13 00-2660 , tanyasm@itu.edu.tr

some RFID tags can cost several dollars, the cost of cheapest ones decreases day by day. It is expected that the cost of Class 1 RFID tags to go down to 15 cents within the next two years. EPCglobal classifies the RFID tags into five main groups such as Class 0, 1, 2, 3, 4 according to its functionality (Roberts, 2006). The classification is shown in Table 1, Class 1 type is the discussed one for global supply chain adoption due to its cost. Manufacturers of RFID tags achieved to produce a tag at 30 cents cost for these class 1 tags (Hou, 2003). Such improvements in cost and size will ensure speedy expansion of RFID technology into many areas of use. For instance to this incredible development of RFID technology, retailers insist on expanding the use of tags from pallet-level to item level (Flint, 2006).

Table 1: Tag Classes according to EPCglobal.

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

Beside the utilities provided by RFID, there are also drawbacks. The great efficiency gains offered by RFID systems may come at cost of inadequacy of privacy, security and standardization issues.

The risk of being read of insecure tags by unauthorized readers is the main concern about privacy and security. Physical attacks, traffic analysis, eavesdropping, counterfeiting, spoofing, replay attacks and denial of service are threats of RFID systems in privacy and security respect (Henrici & Müller, 2004). Each of these risks may affect the privacy and security of both individuals and organizations. When we consider the risks towards individuals, the main risk about privacy is insecure tagging of individual items. Unfortunately, the universal deployment of low-cost RFID tags in consumer items increases day by day. Clothing, shoe and accessory makers have all started embedding RFID tags in their products (http://www.rfidjournal.com/article/articleview/272, 2002). There are some protests against the item level tagging without informing the consumers (http://www.spychips.com). One of the largest clothing manufacturers of the world had to retreat because of boycotts from its customers (Roberti, 2004). Consumers may not even be aware that they are carrying RFID tags. In response to this unawareness, some regulations such as “Bill of Rights” are proposed (Garfinkel, S. 2002). Due to the possibility of being everywhere, RFID tags have the capability of monitoring every detail that you do, what you buy, pretty soon where you go. Retail markets can come to learn the buying patterns of consumers. There are several retail projects being developed nowadays. The concern of these projects happens to be simply tagging store loyalty cards, in order to develop on-line and one-to-one advertisement in retail shops. Another purpose is to determine which parts of the store are being visited most often (or not at all) (Flint, 2006). By means of these studies, digital maps of retail markets can be drown with CRM studies.

Insecure tag threats are not limited to violation of individual privacy. It also threatens organizations. Corporate spies could monitor insecurely tagged inventory of a retail store, a warehouse or a cross-dock. Through periodical monitoring, they can get the sales data or promotions data easily.

Standardization is an important issue as much as privacy on RFID technology. One of the obstacles laying in the future enhancement of RFID is lack of standardization. There exist organizations that have studies on standardization issues such as ISO and EPCglobal. Standardization is important for an enhanced use of RFID through the global supply chain for three main reasons (Yu et al., 2005). First of all, provided that RFID technology has international standards, interoperability across national borders will be achieved (appropriate to global supply chain adoption). Harmonization of standardized tags and readers manufactured by different vendors can be obtained. The other reason for getting the advantage of developing international standards is bringing the costs of exchangeability down. Finally an internationally accepted RFID standard will facilitate the growth of the worldwide RFID market. In spite of all progress on paving the way for RFID usage throughout the global supply chain, there still exist gaps on standardization. As it will later be explained in detail, just after

arriving a compromise on an air interface protocol proposed by EPCglobal (called Generation 2), new debates are about its insufficiency. It has been claimed that Gen 2 can not meet the requirements of item-level tracking: Gen 3 is on its way (Ashton, 2006).

In the following chapter, after determining fields of standardization studies such as air interface, application areas, etc., we discuss the recent standardization studies. In Chapter 3, we go into details in privacy issues, then classify the privacy proposals according to some attributes. Finally, Chapter 4 offers a conclusion and suggestions about the standardization, privacy and security.

2. Standardization for RFID Adoption

As we mentioned previously, standardization is an important issue for proliferation of RFID technology throughout the global supply chain for three main reasons. In summary by courtesy of standardization studies, the interoperability of tags manufactured by different vendors can be provided, the costs of exchangeability get down and also world-wide standardization make RFID usage more common. International Standards Organization (ISO) and EPCglobal are working to develop international standards for RFID technologies especially in UHF spectrum. Even though it is commonly defended that there are no standards or there is no harmonization between existing ones, there are currently many well-established standards. But the completion of all standards can not be achieved up to now. The lack of a complete and unified RFID standard has caused many companies to hesitate in adopting the RFID systems; some companies did not dare to make a commitment to a not standardized technology, by fear of finding one day the whole investment worthless. After mentioning well-established standards, emerging standards such as Gen 3 protocol are also discussed below.

2.1. Fields of Standardization

Standardization studies deal with the description of data link, physical and application layers (Knopse & Pohl, 2004). Data link layer includes anti collision, initialization, data content and tag addressing protocols. One of the distinctive properties of RFID is multiple simultaneous reading of tags (mentioned in chapter 1). Related with this property, simultaneous transmissions on the same frequency may result interference that is called *collision*. Collisions may result in a failed transmission. A method that is employed by readers and tags needed to avoid collisions, referred as an *anti-collision algorithm*. Several attributes can be used to evaluate the quality of anti-collision algorithms (Weis, 2003). These are: performance, range, bandwidth requirements, implementation costs, noise and error tolerance and finally security of algorithms. Anti-collision algorithms may be either probabilistic or deterministic. The most common used deterministic algorithm is called “binary tree walking algorithm” and it is commonly used on UHF spectrum. ALOHA scheme is another well-known algorithm as a probabilistic anti-collision algorithm. Tags operating on highly regulated 13,56 MHz band tend to use probabilistic network. Data content determines how data is organized or formatted.

Physical layer includes air interface functions. Air interface protocol deals with how a transponder is activated and how the information stored in the transponder is transferred to a transceiver. Shortly, it shows the way tags and readers communicate (http://www.rfidjournal.com/article/articleview/1335/1/129/). Instead of anti-collision, air interface protocols have to be standardized.

Application layer organizes how standards are used on shipping labels. Conformance is another protocol of that layer; it deals with testing whether the products meet the standard or not.

2.2. Established Standards on RFID

As a long standing organization, ISO has created RFID standards for many areas like cattle tracking or payment systems (Knopse & Pohl, 2004). ISO 11784 that defines how the data structured on tag, ISO 11785 that defines the air interface protocol, ISO 14223 and ISO 18000-2 are all related with the standards of animal tracking. Only ISO 14223 becomes different from others with further allowance of read/write and write-protected data blocks. These standards are all related with each other and for animal identification in the frequency band below 135 kHz. ISO 14443 has been created for payment systems and contactless smart cards (proximity cards) and they can be operated at approximately 10 cm distance from the reader; ISO 15693 has been created for vicinity cards to define air interface, anti collision and transmission protocols. ISO 18092 defines the near fields communication protocol in the frequency band of 13,56 MHz. For testing the conformance of RFID tags and readers to a standard, ISO created ISO 18047, and ISO 18046 for measuring the performance of RFID tags and readers. ISO has also developed standards for item management. ISO 18000

defines the air interface, collision detection mechanisms and the communication protocol for item tags in different frequency bands. There exists seven parts in this item management standard. First part (ISO 18000-1) is related with the reference architecture. Other parts (2 to 7) specify the characteristics for different frequencies. ISO 18000-2 specifies low frequency tags (<135 kHz). ISO 18000-3 is for HF systems (13,56 MHz) that is compromised with ISO 15693 created for vicinity cards. ISO 18000-4 specifies 2,45 GHz systems; ISO 18000-5 specifies 5,8 GHz band. Part seven (ISO 18000-7) specifies an RFID system with active transponders and range in the 433 MHz band. ISO 18000-6 organized the air interface for 860 MHz to 930 MHz. This sixth part is the most common-known part for two reasons. First of all at this band level, there is no standardization between continents. The United States and Canada allocate the frequency band from 902 to 928 MHz for UHF RFID systems because their GSM bandwidths are not located within this band. The European Telecommunications Standards Institute (ETSI) has released a 2MHz band ranging from 865.6 to 867.6MHz for Europe's UHF RFID use in July 2004 (Word & Kranenburg, 2006). Japan has allocated a 2MHz UHF band ranging from 953 to 954MHz for RFID use in May 2005. The diversity in national spectrum allocation for RFID adds more barriers to the growth of RFID systems in the world market. RFID tagged goods traveling across borders, respond only to a specific UHF frequency range. So the tags cannot be read in countries where different spectrum bands are allocated for RFID use. Secondly EPCglobal's Gen 2 standard is related with ISO 18000-6 for addressing the same application level. The harmonization studies had gone on from December 2004 to July 2006.

EPCglobal is established by EAN International and Uniform Code Council (UCC) to commercialize EPC technology that is developed by MIT Auto-ID Center in November 2003. MIT Auto-ID Center was set up in 1999 to develop the Electronic Product Code and related technologies that could be used to identify products and track them through the supply chain. EPCglobal has the responsibility for commercialization and management of Electronic Product Code (EPC) system researched and developed by the MIT Auto-ID center. Auto-ID Center chose to create its own air interface (UHF) protocol for tracking goods through the international supply chain that is available royalty-free to manufacturers and end-users, instead of using ISO protocols as the standard for the air interface. The reason for rejecting ISO standards is its complexity: it increases the cost of the tag unnecessarily. Cost issue is extremely important for EPCglobal because of its mission, which is to develop a global RFID system that can be used on open supply chains. The tags must be disposable. So the developed RFID system must be a low-cost system. Consequently, Auto-ID Center standardized the air interface protocol at ultra-high frequency band. Only UHF band provides the read range needed for supply chain applications, such as reading pallets coming through a dock door.

In 2004, EPCglobal started to develop a second generation protocol, called Gen 2. The purpose of the studies is to create a single, global standard that would be more closely aligned with ISO standards. EPCglobal approved Gen 2 in December 2004. Afterwards, ISO required revising the protocol in accordance with ISO RFID standards. Unfortunately, the approval of ISO delayed for a disagreement on Application Family Identifier (AFI). EPCglobal finally announced that ISO incorporated its Generation 2 RFID air interface protocol into ISO 18000-6 standards on UHF in July 2006 (Elamin, 2006). Surely, this evidence is a significant milestone in the history of RFID adoption.

TOBB-GS1 is an organization aiming to standardize the national UHF bandwidth in Turkey. It is expected that The Turkish Telecommunications Standards Institute sets the national UHF bandwidth of Turkey as the same frequency band of Europe.

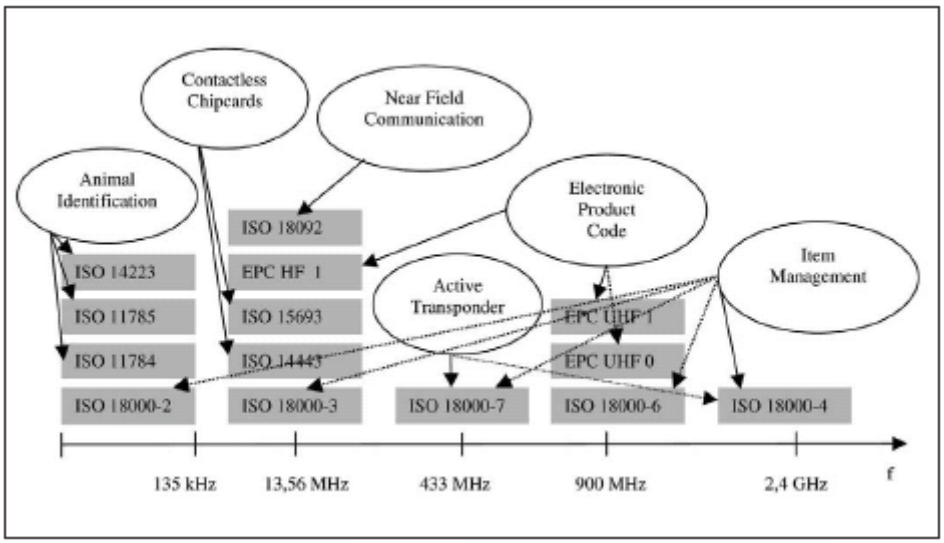

Figure 1: Established standards on different bandwidths (Knopse, H. & Pohl, H. 2004)

3. Privacy & Security

Defined as the ability of an individual or group to keep their lives and personal affairs out of public view, or to control the flow of information about themselves (http://en.wikipedia.org/wiki/Privacy), privacy is an important matter of modern community. According to some authors, improvements in technology are not all for the furtherance of public welfare. For instance, we are regularly filmed by CCTV cameras integrated with facial recognition software. Anyone could follow us through public areas by the help of this devices and software. This example may be considered as violation of individual privacy, to be more specific, a type of privacy called "location privacy". As one might guess, there are different classifications of privacy categories. In this paper we present only two of them. As reported by Weis, the Electronic Privacy Information Center (http://www.epic.org.) categorized privacy into four separate but related groups:

1. *Information Privacy:* Involves rights regarding the handling of personal information such as tax, medical or purchase records. Also known as "data privacy".
2. *Bodily Privacy:* Concerns the right not to be subjected to invasive bodily procedures such as cavity searches and blood, urine or genetic tests.
3. *Communication Privacy:* The right to communicate with others in secrecy.
4. *Territorial Privacy:* Rights limiting intrusion into domestic, workplace or public environments, including searches, identification checks and video surveillance.

According to the other classification type of privacy (http://en.wikipedia.org/wiki/Privacy) there are three main categories:

1. *Political privacy:* The right of keeping your political opinion secret for a variety of reasons - political groupings may be able to commit violence either when successful (using the powers of the state) or when defeated (using their own militias for example).
2. *Medical privacy:* The right of keeping your state of health secret. The reasons for keeping medical information private may include possible discrimination against people with a certain medical condition
3. *Genetic privacy:* The concept of "genetic discrimination" and the associated need for confidentiality of genetic information, or "genetic privacy constitutes this privacy title.

Up to here, we have mentioned the privacy issues and introduced how technology and privacy are related. Hereafter we can evaluate the RFID technology with that point of view. In some cases RFID threatens some of privacy rights. When we assess the risks according to the categorization of EPIC, we can list these threats. Monitoring a warehouse illegally by RFID readers and getting a company's inventory data may violate the right of information privacy. Unauthorized tracking of a persons' state of health by RFID readers also violate the bodily privacy. Tracking cars by RFID technology can also violate the territorial privacy. The government of UK

is working on a project aiming to build a database of exactly where the 28 million vehicles on the road were at any time (http://www.e-plate.com).

3.1. Classification of Proposals on Privacy & Security Issues

While RFID technology is spreading out, the number of studies on security and privacy is increasing. Although some approaches have been fixed in literature, newly developed schemes are being added day by day. Some fixed proposals are given in order:

- Kill Command Approach: By sending a special "kill" command, a tag can be deactivated or killed. A killed tag can never be activated after sending this special command. It is the most straightforward approach for protecting end-consumer privacy. On the other hand it also limits the utilities that can be gained in home applications like smart oven or refrigerator. Major manufacturers of home appliances are working on R&D projects with huge budgets. From this point of view, kill command approach is not so favorable for mass usage.
- Faraday Cage Approach: Using containers made of metal mesh or foil that are impenetrable by radio signals is the general definition of this approach. As one might guess, this method can only be used for valuable goods.
- Active Jamming Approach: The consumer uses a radio frequency device that could create a noisy environment by broadcasting radio signals at random. For purpose of preventing unauthorized readers to get the tag data, this approach could also block other legitimate RFID readers. Because of the drawback, this method is somewhat crude.

Beside these approaches more developed and detailed schemes appear in literature every day. Some of these studies build up on regulative proposals such as "Bill of Rights". Others stress on more technical proposals such as cryptography and authentication. In this study we classify related studies into two main groups: regulative and technical approaches.

3.1.1. Regulative Proposals

Item level tagging of goods increases and so does the possibility of monitoring individuals. The unawareness of consumers that they are carrying RFID tags runs a risk towards individuals. For example, one of the major tire manufacturers of the world announced that they are working on a project about embedding RFID tags in their products (http://www.rfidjournal.com). Most of the people purchasing these tires will never know, nor even suspect, that their car could be tracked by transponders in their tires. Consumers should have some options about buying RFID tagged ones or non RFID tagged ones. Beside the awareness rights, consumers should also have the right of removing or destroying tags on the goods that they purchased. Considering these issues, Garfinkel wrote a "RFID Bill of Rights" (2002) based on the US Department of Health and Education's Code of Fair Information Practices. According to Garfinkel's Bill of Rights:
Users of RFID systems and purchasers of products containing RFID tags have;

1. The right to know if a product contains an RFID tag.
2. The right to have embedded RFID tags removed, deactivated, or destroyed when a product is purchased.
3. The right to first class RFID alternatives: consumers should not lose other rights (e.g. the right to return a product or to travel on a particular road) if they decide to opt-out of RFID or exercise an RFID tag's "kill" feature.
4. The right to know what information is stored inside their RFID tags. If this information is incorrect, there must be a means to correct or amend it.
5. The right to know when, where and why an RFID tag is being read.

The first right may be satisfied using an industry standard logo on all consumer goods carrying an RFID device, such as other similar logos that exist for organic or genetically-modified products. This logo will simply state that the product has the RFID tag, offering consumers the possibility to make an informed decision and decide whether to disable the tag or purchase a non-tagged alternative. This makes the second and third rights practical.

Likely to "Bill of Rights" study, EU is also working on to provide secure environment with RFID usage. In January 2005, the EU Article 29 Working Party on Data Protection issued a "Working document on data protection issues related to RFID technology" and invited comments, the summary of which was published on 28 September 2005 (Flint, 2006).

3.1.2 Technical Proposals

In general there are two technical approaches aiming to provide data security on the RFID tag (Hui, Wong, Chan, 2005). Encryption of the data that is stored on RFID tags is one approach. Authentication between the RFID readers and tags is the other.

3.1.2.1 Cryptographic proposals

Cryptography is defined as a process associated with scrambling plaintext (ordinary text, or clear text) into a cipher text (a process called encryption), then back again (known as decryption) (http://www.stallion.com.au). In this approach, by the encryption of the data stored on the RFID tag, the data can be protected in cipher text format instead of clear text format. By means of this, the data retrieved by unauthorized readers will be meaningless, unless they are able to decrypt all the information they received.

There exist different cryptographic approaches for RFID security issue. The most common-known cryptographic approaches are public key, hash function (lock) and randomized hash function approaches. In public key approach, each tag should carry a particular vendor type of readers' public key and its unique private key. During reading, readers and tags may mutually authenticate each other with these embedded keys. Authentication between readers and tags can be achieved by a challenge–response technique. Eavesdropping can be prevented unless attackers find out the actual private key of each tag, but this is unlikely in a short period of time. In hash lock approach, a tag may be locked so that it refuses to reveal its ID until it is unlocked. In the simplest scenario, when the tag is locked it is given a value (or meta-ID) y, and it is only unlocked by presentation of a key or PIN value x such that $y = h(x)$ for a standard one-way hash function h. Randomized hash function approach is an extension of hash lock approach. The main difference is based on pseudo random functions. An additional pseudo-random number generator is required to embed into tags for this approach. Presently, tags respond to reader queries by a pair of values (r, hash(IDk || r)) where r is the random number generated by a tag, ID_k is the ID of the k^{th} tag among a number of tags in ID_1, ID_2, ..., ID_k, ..., ID_n. When a reader inguire the tag, it gets two values: a random number and a computed hash value. Computed hash value is based on the concatenation (||) on its own ID_k and r. If the reader is an authorized one, it can check all registered ID values on its backend database and finally reach the ID_k value for that specific tag . Thanks to this process, tag authentication can be provided. After sending the ID_k to the tag, tag will be unlocked and send its EPC data.

After introducing these three major cryptographic approaches, we can compare these according to their drawbacks. Public key approach necessitates high computation power for RFID tags. Thus, the cost and also the size of RFID tags are greater for item-level tagging. The main disadvantage of hash function approach is the lack of mutual authentication. For example, a hacker can obtain the Meta-ID value of a tag, then with this value, he/she can counterfeit a tag and can get the specific random key from the authorized reader for this Meta-ID value. Therefore, the hacker can catch the chance to get the key to unlock the tag and obtain its EPC data. Besides the hacking possibility, hash function approach can not provide the location privacy due to the stable Meta-ID value broadcast by the tag. As one might guess, randomized hash function is more reliable for privacy and security respects but it is not practical or feasible for systems that have big numbers of tags. Because of the random number generator, the cost of tags is high.

3.1.2.2 Authentication proposals

Normal information retrievals from the tags to the reader can be allowed to proceed, provided that authentication has been done before. Thus, both the reader and the tags identify they are the right parties to exchange information. In order to prevent illegal access to the memory segment of tag, there should be a procedural access control. In literature there exist studies on authentication proposals that are mentioned in the next part of this paper.

3.2 Summary of Proposals on Privacy & Security Issues

When the studies related with security/privacy issues are examined one by one, it can easily be seen that most of them focuses on EPC Class 1 RFID systems. The main reason is that it is targeted to use Class 1 tags for global supply chain adoption thanks to low costs. Related with this cost attribute other constraints exist on Class 1 tags. Their computational capacities, memories and read-write storages needed for cryptographic and authentication processes are limited. Class 2, 3 or 4 types of tags have the capability of supporting any complex

cryptographic protocols. So it is easy for these systems to provide secure environments, but on the other hand these systems are too expensive for mass markets.

Henrici and Müller developed a simple hash based scheme to overcome limited tag resources (2004). They aimed to keep only short-term values in a tag. The main data storage work is loaded to back-end database system. Their scheme is based on a one-way, simple hash function and a key management process executed on backend system. Although the tag only performs hashing, location privacy can be provided by changing the Meta-ID of the tag in every read attempt. This means that the tag changes its identity on every query. A structure called reference database manage these procedure of identity changing. The database must provide a single random number to calculate the new tag identifier. In this scheme complex processing is required neither at the tag nor at the database. This proposal is favorable for its simplicity. It only requires implementation of a hash function in the tag and data management at the backend. It does not necessitate random number generation on tags. Location privacy is also provided. It is claimed about the scheme developed by Henrici and Müller that it can not resist to replay attacks (Chien & Chen, 2006).

Juels, Rivest, and Szydlo (2003) added a new approach for protecting consumer privacy to the conventional classification mentioned in 3.1. In addition to kill tag, faraday cage, active jamming approaches, they put forward "smart RFID tag" approach. They mixed hash-lock approach and re-encryption approach in this title. In addition to these, silent tree walking that is mentioned previously as an anti-collision algorithm is considered in smart RFID tag. The scheme developed by Juels et al. is the mixture of active jamming and tree-walking protocols. As mentioned before active jamming approach is a crude approach. It could cause severe disruption of all nearby RFID systems, even those in legitimate applications. However the proposed approach is akin to jamming, but it is more clever in its operations by interacting with the tree walking singulation algorithm. It aims selectively blocking. This approach uses tree-walking singulation algorithm for two reasons: tree walking algorithm is likely to be the most common anti-collision technique, and also it is supportive of the more flexible modes of blocking. As cited above, there is one more well-known singulation approach called ALOHA. However the proposed smart blocker tag technique does not work with ALOHA, since it is not possible to block certain subranges of IDs on a selective basis. Selective blocking can materialize by tree-walking algorithm with the feature of simulation of the full set of 2^k possible RFID-tag serial numbers conducted by blocker tag. The tree-walking singulation algorithm enables an RFID-tag reader (also enables the blocker tag) to identify the serial numbers of nearby tags individually by means of a bit-by-bit query process resembling a depth-first search of a binary tree.

For example, in Figure 2 a tree which is of depth 2 is shown. So it has $2^2 = 4$ tag serial numbers represented in its leaves. If only two of them are present, the others are only imitated two-bit serial numbers. This means they refer nothing. An unauthorized reader can not know which ones do really exist.

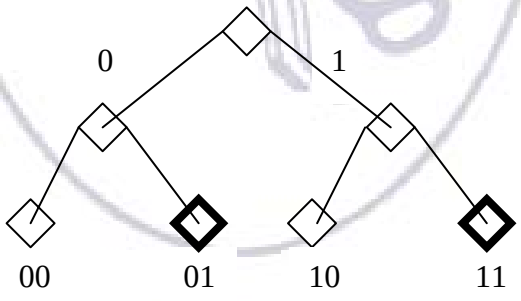

Figure 2: A depth-two binary tree. (01 and 11 tags are present)

Considering that an EPC code consists of 64 or 96 bits, it is hard for an unauthorized reader to inquire each 2^{64} or 2^{96} alternatives. In selective blocking tag approach, a blocker tag simulates the full spectrum of possible serial numbers for tags of a physical region that is aimed to keep private.

The approach developed by Juels et al. is feasible for its very low cost implementation. It is cheap to implement because the RFID tags which are in use in consumer goods may not to be modified at all, and the blocker tag also is cheap. It is a modified version of a standard tag with two antennas that is required to simultaneously broadcast both a "0" bit and a "1" bit.

As mentioned before the studies related with security/privacy issues mostly intensify on Class 1 tags. However a few of these studies are on Class 1 Gen 2 protocol. The main reason is that Gen 2 is approved by ISO recently (in July 2006). The scheme proposed by Chien and Chen is one of the three studies related with Gen 2 tags in literature (2006). The others are Karthikeyan-Nesterenko's scheme and Duc et al.'s scheme. After stating the reviews and weaknesses of these two studies, Chien and Chen present their new mutual authentication protocol. As mentioned by Chien and Chen, Gen 2 RFID tags cannot support any hash functions due to their limited resources. So the other proposals mostly cannot be implemented on Gen 2 RFID tags in security respect. The proposed scheme consists of two phases: initialization phase and authentication phase. Due to the challenge and response technology and the freshness of random numbers, proposed scheme is reliable. Only the randomized data is transmitted on the wireless channel between the reader and the tag, and the product information (EPC) is only transmitted from the server to the reader through the secure channel.

Ayoade recommend the scheme called Authentication Processing Framework (APF) as a feasible method to overcome privacy and security problem (2005). According to this method both readers and tags must be registered to APF database. This framework makes it compulsory for the readers to authenticate themselves with the APF database before they can access registered tags. The data stored in the tag is encrypted. To get the data from the tag, the reader needs to have the access (decryption) key of tags that is registered in APF database. It is difficult for any reader to have access to the memory segment of the tag without possessing the access key. Only authorized readers that were determined when they were registered to APF with their unique identification number reach the EPC data. This framework can not be suitable for global supply chain applications, due to the enormous data management load. It is not feasible to register all tags and readers to a database in a global supply chain. But in limited application areas it can be useful. Ayoade applied his framework on a particular area in a real world system. This area was patient confidential/personal information area. By the APF system the information about a patient stored in an RFID tag attached to his hospital card can only be seen by his doctor or related staff.

Hui et al. proposed a new approach in their study (2005). Their study differentiates from others and makes itself more reliable for having both real applications and also performance tests performed comparatively with a well-known cryptography scheme (DES algorithm). The proposed scheme consists of two phases. In the first phase the EPC data stored in the tag is encrypted by a heuristic Jigsaw encoding scheme. This helps to encrypt an EPC data into a pseudo-EPC code. An unauthorized reader can not reverse the pseudo-EPC code into a valid EPC code in a short period of time. The reader has to get the scattering way of Jigsaw Algorithm. Without the knowledge of the scattering way to a matrix, it is not possible for attackers to resolve it in a short time because it involves a permutation of 64 ways. In the next phase, a simple tag authentication scheme is proposed by using a one-way hash-lock function. By this step it will be realized that the tag is cloned or not. After developing the scheme, it is tested for implementation. Jigsaw algorithm is compared with DES algorithm which is the most well-known algorithm. Two hundred measurements were made to execute cipher operations on a 64-bit EPC tag. First comparison attribute is time for encryption and decryption. Jigsaw algorithm is obviously faster than DES. Jigsaw is more appropriate for ease of use and efficiency. These two algorithms are at the same operational reliability level. Even DES is more secure, Jigsaw is more feasible to apply according to all other criteria. The scheme is designed for the application on EPC Class 1 Gen 1 protocol and to be used with apparel products.

4. Conclusion

Important acquisitions in many application areas are gained by RFID technology. There are still R&D studies and debates going on in order to enhance the functionality of this technology. The main purpose of the studies is to provide international standards and find a solution for consumers' privacy and security problems. Due to the promises made by RFID technology on numerous fields and applications, the studies on RFID standardization and privacy issues vary. Whereas some security/privacy proposals are focused on providing consumer security in particular application areas such as hospitals, others also turn to global supply chain applications. Similarly, the differentiation can be related with tag classes. While new proposals for Class 1 Gen 2 tags are being introduced, schemes for Class 1 Gen 1 type tags are also being developed. From this point of

view, one can easily say that no single proposal is likely to be completely satisfactory. For the purpose of finding the most appropriate scheme, there exist some criteria that must be considered, which are:

- Application area (open supply chain, or a more specific area such as a health facility),
- Type of tag (considering its capabilities such as computational load, memory capacity),
- The degree of desired operational reliability, performance, operation time and ease of use.

Performance tests must be conducted in order to find the best scheme for that specific application area. Sometimes combination of methods may prove to be the best.

5. References

Ashton, K., 2006. The history of EPC's future. ***RFID Journal***, March-April Vol. 3 No. 2.

Ayoade, J. 2005. Security implications in RFID and authentication processing framework. ***Computers & Security,*** (2006).

Chien, H., & Chen, C. 2006. Mutual authentication protocol for RFID conforming to EPC Class 1 Generation 2 Standards. ***Computer Standards & Interfaces,*** 2006.

Elamin, A., 2006. ***EPCglobal RFID standard accepted by ISO.*** http://www.foodproductiondaily.com/news/ng.asp?id=69309-epcglobal-rfid-supply-chain

Flint, D. 2006. RFID tags, security and the individual. ***Computer & Security Report,*** 22 (2006) 165-168.

Garfinkel, S. An RFID Bill of Rights. ***Technology Review***, page 35, October 2002.

Henrici, D., & Müller, P. ***Tackling security and privacy issues in Radio Frequency Identification devices.*** In submission, 2004.

Hui, P., Wong, K., Chan A. 2005. Cryptography and authentication on RFID passive tags for apparel products. ***Computers in Industry,*** 57 (2006) 342-349.

Hou, C. H. 2003. ***Quick and easy payment***. http://computertimes.asiaone.com.sg/issues/story/0,5104,1795,00.html

Jones, P., Clarke-Hill, C., Shears, P., Comfort, D., & Hillier D. 2004. Radio Frequency Identification in the UK: opportunities and challenges. ***International Journal of Retail & Distribution Management,*** Vol. 32 – Number 3 (2004) 164-167.

Juels A., Rivest, R.L., Szydlo, M. ***The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy,*** 10th ACM Conference on Computer and Communication Security, 2003.

Knopse, H. & Pohl, H. 2004. RFID Security. ***Information Security Technical Report***. Vol. 9, No.4.

Roberti, M., 2004. ***New rules of the game.*** http://www.rfidjournal.com/article/articleview/820/1/2/

Roberts, C. M. 2006. Radio Frequency Identification (RFID). ***Computers and Security,*** 25 (2006) 18-26.

Weis, S. A. ***Security and privacy in Radio Frequency Identification devices.*** Master's thesis, M.I.T. May 2003.

Word, M. & Kranenburg, R. RFID: Frequency, standards, adoption and innovation. ***JISC Technology and Standards Watch***, May 2006.

Yu, H.C., Wu, N.C., & Nystrom M.A. 2005. ***Challenges to global RFID adoption.*** Technovation***.***

http://en.wikipedia.org/wiki/Privacy

http://www.e-plate.com

http://www.stallion.com.au

http://www.epic.org/privacy/rfid/

http://www.spychips.com/

A summary of RFID standards. http://www.rfidjournal.com/article/articleview/1335/1/129/.

http://www.rfidjournal.com/article/articleview/272, June 24, 2002.