GRBER Global Review of Business and Economic Research
Vol. 9 • No. 2 • Autumn 2013 : 175-186

LEGAL AND SECURITY MEASURES TO BE APPLIED TO THE NEW GENERATION OF THE RFID SYSTEM

*Eva El Haj Chehade**

Abstract: *The Radio Frequency Identification (RFID) technology is used from a long time in the identification of tagged items. Nowadays, the usage of the RFID technology is expanded in the business field, especially in improving supply chains by introducing the EPCglobal network, the leader in managing the standards of the Electronic Product Code (EPC). The new generation of the RFID system, as we discussed later on, makes the system universal with some added features like the ownership identification, the part-assembly association and the maintenance documentation. The technical implementation, as it was discussed later, ensures the validity of the new system but needs to be empowered by some controls; legal and technical. Legal controls obligate the users to realize the system characteristics. Technical controls are presented by the security measures. To secure the network; Firewall, Virtual Private Network (VPN), and Intrusion Detection System (IDS) will be implemented. Thus, our research will be based on the implementation of theses controls.*

Keywords: Radio Frequency Identification, Electronic Product Code, Firewall, Virtual Private Network, Intrusion Detection System.

***Field*:** *Management Information Systems*

1. INTRODUCTION

The RFID technology starts from decades by the identification of items, and is improved with time to be introduced in our daily life and in the business field. The RFID technology plays a main role in the business sector by improving supply chains. This was done due to the EPCglobal network proposed by EPCglobal, the leader in developing standards for the RFID Technology.

Thus, the EPCglobal network is very useful in the business world and has a main role in improving the supply chain management, but still limited to the supply chain and can not follow part items leaving their supply chain to join another chain in order to be incorporated in the assembly items. The new generation of the RFID system, as we have explained, has an effective contribution in improving the RFID system. The added value applied to the new RFID system is characterized by the system universality, the ownership identification, the part-assembly

* University Institute of Technology, Lebanese University, *E-mail: eva.hajchehade@gmail.com*

association, and the maintenance documentation. The technical implementation of this new generation of the RFID system needs to be managed and controlled in a way that ensures benefits for the manufacturer and the user at the same time. For this reason, many controls have to be added such as legal controls and technical controls. Legal controls are applied to force users of this new system to ensure the system features. This can be done by making all the adjustments in the data base concerning the change of the owner or the part items, or concerning the maintenance operations. This will help the system to reveal the reality. Technical controls are presented by the security measures applied to the system. Security measures will concern the tag, the reader, the data base, and the network.

Different scientific papers, articles, researches and literatures have been discussed to analyze the RFID technology, and especially the EPCglobal network, their legal and technical controls, and their security aspects. A new generation of the RFID system and its business value in our days has been exposed by Eva El-Haj-Chehade, Akram Tannir, and Abdul-Nasser El-Kassar (2009). Moreover, the technical implementation of this new generation was also proposed by Eva El-Haj-Chehade, Akram Tannir, and Abdul-Nasser El-Kassar (2012). On the other hand, many papers exposed the technical, legal and security controls applied to the RFID system and that can be beneficial to be applied for the new generation of the RFID system. Thus, Sadeghi (2009) presented instructions and requirements for security and privacy of RFID systems that are compatible with legislations. Recently, Shaoying Cai (2010) introduced a secure protocol for tag transfer in RFID supply chains. Furthermore, Mitrokotsa (2009) classified RFID risks and attacks and discussed their features in order to develop algorithms and procedures that might be suitable to face these attacks. Moreover, Shaoying Cai (2009) evaluated the security measures and classified them into two levels (strong and weak), where the weak security mode allows RFID systems to be managed in highly efficient manner and the strong security mode provides a higher security level and lower efficiency level. In this study, many protocols are presented to facilitate the dual security mode. However, privacy concerns and policies have been examined by Namje Park (2008) in order to propose RFID solutions protecting user's privacy. In addition, Namje Park (2008) described a secure RFID framework based on web service. Lehtonen (2009) focused on determining the mathematical model of the method used to prevent RFID systems from tag cloning. The hardware implementation of RFID security algorithms has been reported and a comparative study of these algorithms was analyzed by Martin Feldhofer (2008).

In the following section, the existent legal controls will be analyzed in order to improve these existent policies in a way that makes them compatible with the new proposed system. Section 3 will describe all the technical controls presented by the security measures that should be applied to the new system. This is done at all the levels of the system starting by the tag, the reader, the database, and

concluding by the network as whole. Finally, in section 4, a summary of all what we are explained will be reviewed and a vision of future possible research will be presented.

2. THE LEGAL CONTROLS

The EPCglobal is responsible for developing and publishing of RFID tags standards that are considered to be useful and effective in order to reach a set of specifications that are common and that enable manufacturers as well as end users to use an interoperable system that controls the making and the use of the RFID tags. Moreover, the EPCglobal offers an open use of the EPC network while still protecting its integrity.

Thus, the EPCglobal has established a set of rules for the EPC construction as well as its architecture. These rules are in fact a set of particular technical specifications which have been acknowledged by the working group and accepted by the trustees. In addition, the EPCglobal has opened up the chance for participants to take part in the development of EPCglobal standards through the EPCglobal's Action and Working Groups. Thus, the EPCglobal has issued a declaration which is a binding agreement as well as a required admission for participating in these groups. Hence, companies that wish to enroll need to sign the adequate EPCglobal Intellectual Property (IP) Policy and forward it to the EPCglobal affiliate. Furthermore, the EPCglobal Intellectual Property Policy asserts that all subscribing companies have open, neutral access to EPCglobal network technology and standards. At the same time, the agreement ensures that the technology is not considered as a property for any party, but it is rather maintained for the welfare of the industry as a whole.

The current specifications, standards and protocols have been working very well for the system in its current design and function. However, in order for the proposed enhancement to take place, they have to be accompanied with parallel adjustments on the system's protocols, standards and specifications. These adjustments are not only set for the way the system functions, but they also cover the laws and regulations that facilitate the operational procedure of the system's new adjustments.

Hence, in order to organize the operation of the new adjustments introduced into the system, some essential measures need to be taken in order to establish the legal bases upon which these enhancements could come to their fuller realization in the market. Thus, additional laws and regulations need to be formed and enforced in order to safeguard the system's way of operation in its maximum effective capacity. Therefore, this legal coverage for the application of the system takes the shape of legal agreement. Thus, in addition to the existing EPCglobal IP Policy, the legal agreement will holds companies preferring to participate in the

EPCglobal network to be responsible for taking the necessary actions to ensure the application as well as continuation of the system. Hence, these companies, must control the update the data base in order to identify the new owners of the item, link any part items to the assembly item, and help in keeping record of any maintenance procedure that might be done to the item. Therefore, these updates take place by accessing the manufacturer's data base since he is the one who has produced the product and the one who is responsible for tracing it all around.

In addition, the two main parties involved in the legal agreement are then the company participating into the system and the EPCglobal which plays the role of the organizer who monitors the procedure by actually being responsible for shaping the agreement as well as designing its page on the website. Therefore, it will be signed either via website or locally at any EPCglobal affiliate. This operation does not seem to be complex since it is applied for precious and dangerous items that already need the application of some legal rules and protocols.

In addition to the interest of EPCglobal companies to ensure the good application of the system, the purchaser will have also the attention to make all the updates in the data base in order to prove its ownership of the item (the assembly item with all its parts). Moreover, what urges the purchaser to take the trouble and stick to the required procedure of the continuous updating process is the fact that the success of the system provides any consumer or purchaser with the assurance that the product he has purchased meets the high standards set by the EPCglobal for which this later has given its approval. Hence, it becomes an obligation for the purchaser to participate in this procedure in order to guarantee his right of a high quality service.

The main goal for any successful business man is to achieve profit. Moreover, it is then the manufacturer's role to not only produce quality items but also to provide high quality services that are responsible for promoting the business. Thus, participating in the EPCglobal system becomes an inevitable step that business man must take to ensure not only the continuation of his business but also its progress as well as its development.

Therefore, the implementation of the RFID system affects the attitude of the purchasers in the society since it sets the standards for which the manufacturer's products are accepted and trusted by the purchasers. Thus, the EPC tag becomes the label that guarantees the good services that the purchaser looks for to make his purchase.

Moreover, the EPC system does not only help in establishing trustworthy grounds with local purchases, but it also help the manufacturers to market their products abroad since this system is recognized and adopted internationally. Hence, through the EPC system, any manufacturer can gain grounds not only locally in his country but also internationally wherever the EPC system spreads.

3. THE SECURITY MEASURES

The proposed system is based on a delicate framework that depends on the correctness as well as the accuracy of the data which is dealt with as well as the procedures through which this data is being handled. Hence, security measures that ensure the safety of each and every level of the system such as the tag, the reader, the data base as well as the network are mandatory in order to safeguard the success and the continuation of the system in the face of any sabotage attempts by any hacking interception. Therefore, these security measures need to insure the prevention of any possible danger, the detection of the security breach once it occurs as well as the suitable reaction that should be taken to handle the problem as well as prevent it from reoccurring any time in the future. In doing so, the integrity of the system as well as the confidentiality of the data should be maintained and preserved. Consequently, these security precautions would ensure that the data provided is accurate and safe from any manipulation attempts. In addition, the availability of both the data and services provided by the system would also be ensured because of the tight security measures that prevent these services from being attacked or stopped. However, these theoretical requirements need to be transferred into a practical plan of security which includes a set of steps. First, to achieve a security system, there need to be a set of policies that form the basis as well as the guidelines for the strategies through which the security plan is applied. Second, these policies should be translated into practical measures that cover all the levels of the system. The third step would be the implementation phase where the equipments and tools required would be provided and installed. In addition, the various security missions would be distributed to the assigned groups responsible for achieving these missions. However, these steps would not be sufficient unless they were tested against manipulation and intrusion attempts. Hence, these security measures would be put into practical test in order to prove their validity against any sort of security breach. Finally, this security plan requires continuous surveillance and auditing procedures to ensure that nothing wrong takes place, and that no exceptions were made under any condition. Moreover, these surveillance procedures would undergo non stop updating operations in order to maintain the validity and effectiveness of the security policies.

There are certain essential elements that are considered the essence of the security concern. One of these elements is the identification process through which the identity of all those who are using the system is identified. The second element is that of authentication through which every identified member who wishes to access the system would be verified by providing a private password, or by using their biometric authentication methods. Finally, controlling access to the system is also a major element in maintaining the security of the system. Hence, it is quite important to determine the accessing levels for those who are granted access to the system. Thus, the various levels of security that correspond to the different

groups of users need to be established in a way that acknowledges the limits and boundaries for all those who access the system depending on the level of access they are granted.

When looking closely at the existing operational levels which constitute the core of the system, we find that any security plan needs to be designed in a way that covers the four major elements which are the tag, the reader, the data base, and the network.

One effective way to increase the safety level of the tag is to design built in tags since they have the quality of being irremovable as well as unreachable by users. Moreover, this design also facilitates the identification as well as the tracing of the object any time during the life cycle of the product even if it was stolen or lost.

On the other hand, it is essential for our system that the tag used is a passive tag that has unlimited life time period since it does not an internal power supply. Hence, the passive tag is sufficiently powered up by the incoming radio frequency signal so that the integrated circuit in the passive tag would be provided with the necessary power to transmit a response. This would eliminate the risk of losing the power in the tag which leads to the loss of the tag itself. Consequently, the tag will persist all through the life cycle of the product.

Moreover, the tag used in our system must be a read only tag. The tag has different memory types; it can be read only, read/write or even Write Once Read Many (WORM). Using a read only tag prevents the tag from being modified and helps in assuming a higher security level; that is why a read only tag will be used for security reasons.

For the security of the reader, our concern is in preventing illegal reading of the tags. Thus, our concern is with the attitude towards the tag which should not adhere to the "kill command", but should adopt the usage of a guardian device which protects the tag from being read by unauthenticated readers through notifying the owner of such an intrusion.

On the one hand, killing a tag will take a place in a slow physical process that resembles the imprinting process which leaves the tag permanently inoperable. This could be done by disconnecting the antenna, subjecting a fuse to a short electrical current or to high energy microwaves. However, to prevent unauthenticated killing operations, detection units may be installed to detect when tags are disabled. Hence, the tag might produce a scream as a signal burst on a certain frequency to notify such illegal killings.

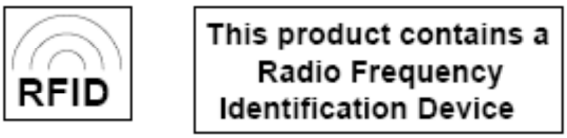
However, killing the RFID tag seems to have many disadvantages. First, the value of the activated tag extends to reach the after sale phase. Hence, killing them would deprive the community from such after sale advantages such as facilitating item returns or repairs. Second, killing them would be a financial loss since it is a

waste of the money and the efforts which were invested on them. Therefore, it would deprive us from the ability to track the product although we had already paid and made all the investment.

On the other hand, the other possible alternative would be using a guardian device with the aim of protecting users' privacy from being attacked. This guardian is a PDA device which could be held in the hand to notify consumers when an RFID scanner is attempting to read a chip by producing a beeping sound. It operates on a 550 MHZ X-Scale 32 bit processor with 64 Mbytes of RAM.

In order to manage the way readers operate, certain policies were issued. These policies organize as well as discipline the manner by which the readers function. First, products that carry RFID tags must be labeled in order to notify the consumer about this fact, see figure I. Second, consumers also are given the right to know what information is stored inside their RFID tags as well as the data base information which correlate to them. Third, consumers are granted the right to know the time, the place as well as the reason why an RFID tag is being read. Other policies include enabling readers to produce a certain tune or to flash a light when a reading takes place. Moreover, the tag itself would produce a tune or a flash light. Finally, a tag that contains a memory could initiate a counting process that counts the times it has been read.

Figure 1: Examples of Labels which could Appear on RFID-labeled Products

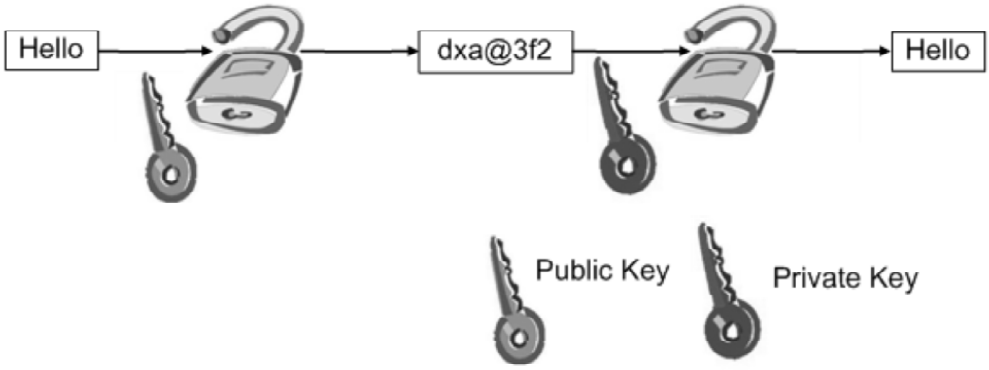


Since the data base is the true basic unit that holds all what is considered to be important information about not only the product, but also the producer or manufacturer as well as the consumer, it is essential then to encrypt the data stored in the data base to prevent any sort of manipulation or intrusion to the information. The aim of this encryption is to ensure that the transmitted data will remain confidential since any attempt to intrude into the system would be futile because the intruders would not be able to interpret the meaning of the information intercepted. In addition, encryption process also helps in safeguarding the integrity of the data against any modification attempts while it is being transmitted. Moreover, encryption also ensures that only authentic members who can decrypt the data would have the ability to interpret as well as make use of the encrypted information.

Data can be encrypted in various ways. Our system would depend on the Public Key Encryption (PKE) since it is both secure as well as practical. The public key

encryption depends on the usage of two keys; one is public and the other is private, see figure II. This concept was developed by Whitfield Diffie and Martin Hellman in 1975 in order to provide a secured key exchange. Every member would have a private key that is accessible by him; however, this same member also has a public key which is revealed to all people without any risk. Hence, when a message needs to be send to a member, the message would be encrypted using the member's public key who will, in turn, decrypt the message using his own private key so that no one else but him would have the ability to interpret this message. Moreover, it is impossible to derive one of these keys from the other.

Figure 2: The Public Key Encryption (PKE)



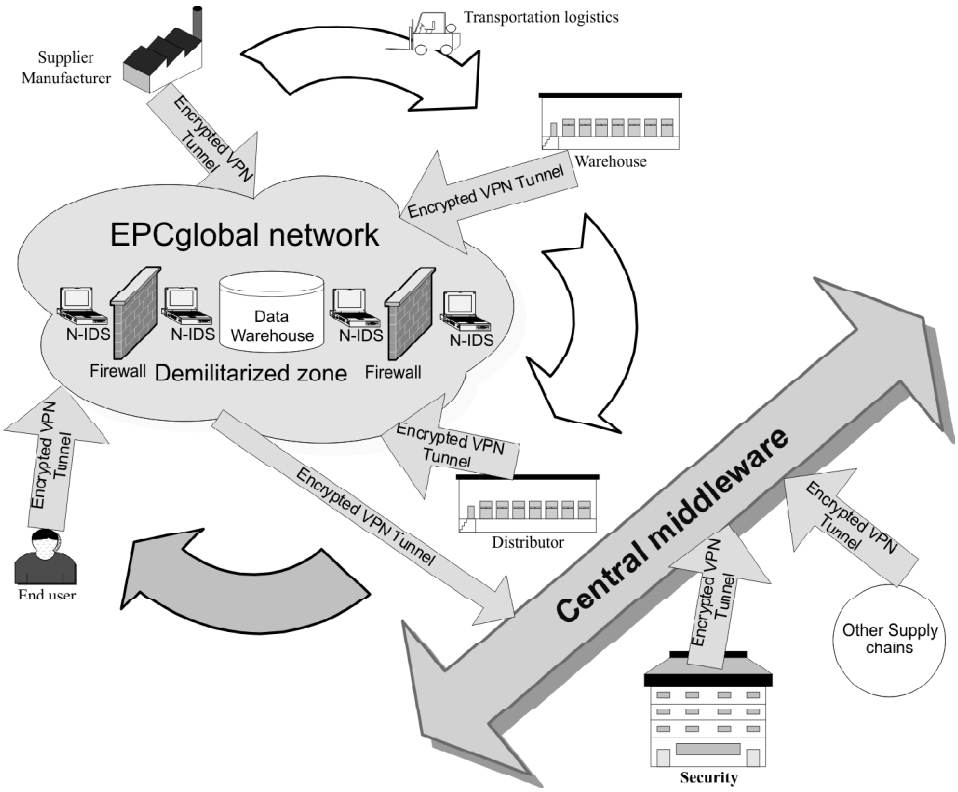
This way of encryption (PKE) has many advantages. First, the exchange of the public key is simple. Second, it is also easy for every one to obtain the public key which makes it quite easy to reach to all the members of the community. Finally, the exchange of the public key takes place in a confidential manner which creates an acceptable level of security.

However, the Public Key Encryption also has some disadvantages. For, the great number of calculation cycles makes the usage of the Public Key Encryption some how complex. In addition, this reality also leads to a bigger consummation of resources. Yet, PKE remains effective enough to benefit our system.

In order to secure the network of the system, we need to take various security measures which are: a Firewall, a Virtual Private Network (VPN), as well as an Intrusion Detection System (IDS) which would help in maintaining acceptable security levels against any hackers or intrusion attempts, see figure III.

A Firewall is a fundamental element in forming a defense line that protects the information technology against any threat that jeopardizes the safety of the data dealt with. Moreover, a Firewall prevents the spread of any sort of attack on the net, and, at the same time, it permits the passage of the traffic of data that is both

Figure 3: The Secured EPC Architecture among Various Supply Chains



authorized and beneficial for the system. It plays an important role in achieving various tasks. First, it filters the data through selecting the needed package of information and allowing it to pass through the system. Second, it is responsible for sending alert to the administration in case any attack occurs. Furthermore, the Firewall achieves this not only for the information that passes in, but it also does it for the package of information that is getting out of the system. However, the Firewall in it self is not enough to ensure the security of the system without careful control and configuration for it. Moreover, a configuration with double Firewalls can build a safe demilitarized zone where all the servers, the data bases, and the data warehouse will be placed in a protected perimeter controlled in all its entrances by the usage of Firewalls. Hence, installing a Firewall is effective when the principles for its installation are set accurately. Therefore, a Firewall needs to be set as to grant each member of the system the minimum privilege of accessibility that is required. Thus, a normal user would be granted an access to the system as a user and not as an administrator. Moreover, a Firewall needs to present a profound defense by utilizing multi-security measures that cover all aspects and not a single one. Furthermore, the Firewall is set to deny the access of all which is not explicitly

permitted instead of permitting the access of all which is not explicitly denied. This procedure is adopted due to the fact that we can not predict what might attack the system in the future; therefore, it would be safer to prevent by default all sort of access. Later on, the access would be gradually granted only to the required traffic of data. It is essential that these principles are respected and preserved by the users. Hence, the principles' effectiveness depends on the users' attitude which needs to be a positive and protective one rather than being illusive or deceitful. At the same time, the system needs to be flexible enough to provide all the needs of the users without forcing a lot of restrictions on them in a way that limits their freedom and stimulates their attempts to break or over ride these principles. Finally, most of the errors that take place result from humans; thus, a simple system would minimize the risks of making mistakes as well as facilitate the ability to monitor its way of operation to ensure that it is working properly.

A Virtual Private Network provides the passage of sensible data through the network while maintaining its confidentiality. It helps in lowering the cost of communication as well as facilitating far distance connection. Moreover, a VPN has some important characteristics. First, the passing data traffic is encrypted in order to maintain the confidentiality of this data. In addition, distant sites will be authenticated in one or two directions. The type of connection used would be a two point connection where one point could be the user and the other a site, or one would be a site and the other is another site. Hence, the type of connection between the different members of the system is a site to site type of connection where as a client who is an end user uses a user to site type of connection in order to perform the required updates. Therefore, in the user to site type of connection, there has to be a management of both the profile as well as the security policy that suits the profile. As for the site to site connection, it is quite beneficial because of its role in lowering the costs of the data transfer as well as the renting costs of the international lines.

An Intrusion Detection System (IDS) allows us to protect the network from any attack. It resembles an alarm that sets off when any theft takes place or even a night guardian against any act of menace. It detects any attempt to access an assigned protected perimeter.

There are two basic types of IDS. The first type is the Host based IDS (H-IDS) where as the second is the Network based IDS (N-IDS). On the one hand, the Host based IDS is installed on a particular host, and it controls the system files, the applications, the modifications done on the files of the system as well as all the access attempts. Therefore, many aspects of vulnerability in the system would be detected and stopped or even put out of service. On the other hand, the network based IDS is generally installed by programming the switch or by using a hub. Thus, the data traffic on the network would pass through the card of the N-IDS. In

addition, the Network based IDS has many attack signals for which updates take place on daily basis. Furthermore, the N-IDS is installed after or before of the Firewall. Hence, when it is installed after the Firewall, it is concerned with any attacking attempts that managed to bypass the existent Firewall where as if it is installed before, then the concern is with controlling the attacks on the entire traffic data.

The N-IDS has many advantages as well as disadvantages. As concerning the advantages; the N-IDS has the characteristic of being completely hidden within the network. Moreover, it also has the ability to control a great bulk of traffic of the system. In addition, it has the ability to capture the content of all the information packages that are sent to the system. The N-IDS has some disadvantages as well. For, its alarming characteristic is restricted to the mere attacking signals that it configures. Finally, the Network based IDS has no ability to identify encrypted traffic which decreases the security level maintained in the system.

In general, The IDS installation requires some measures. First, the security perimeter needs to be accurately defined. Second, the objective of the IDS also needs to be clearly defined. Furthermore, the controlled objects also need to be identified and chosen. In addition, the alarm, the actions as well as the rules need to be clearly defined. Finally, the security policies need to undergo regular updates to ensure its effectiveness.

The security configuration combining the Firewall, the Virtual Private Network and the Intrusion Detection System realize an important level of security assuming a protected system able to facing all kinds of intrusion attacks.

4. CONCLUSION

The controls introduced in this paper will be applied to the new generation of the RFID system. The new generation of the RFID system is presented by the improvement introduced to the EPCglobal network in a way that makes it universal and applicable all over the world over different supply chains, in addition to many features that adds value to the EPCglobal network. The technical implementation of these improvements applied to the existing system is completed by many controls ensuring the usage of this new system for the benefit of the user and the manufacturer as well. These controls are applied in two levels; legal and technical via the security measures. Analytical procedure of the exiting infrastructure is used to apply these controls. Moreover, network diagrams and illustrative pictures are also used.

Finally, inspired from this work, we propose the cost of the implementation to be subject of future research. The cost of the proposed system must be a moderate one in order to help this new solution to be realized.

References

Article

Cai, S., Li, T., Li, Y., Deng, R. H. (2009), "Ensuring Dual Security Modes in RFID-Enabled Supply Chain Systems", *Lecture Notes in Computer Science*, Vol. 5451.

Cai, S., Li, T., Ma, C., Li, Y., Deng, R. H. (2010), "Enabling Secure Secret Updating for Unidirectional Key Distribution in RFID-Enabled Supply Chains", *Lecture Notes in Computer Science*, Vol. 5927.

El-Haj-Chehade, E., Tannir, A. and El-Kassar, A. (2009), "The Business Value of the New Generation of the RFID System", *Review of Business Research*, Vol. 9, No 1, pp. 56-67.

El-Haj-Chehade, E., Tannir, A. and El-Kassar, A. (2012), "The Technical Implementation of the New Generation of the RFID System", *Global Review of Business and Economic Research (GRBER)*, Vol. 8, No 1, pp. 35-51.

Feldhofer, M., Wolkerstorfer, J. (2008), "Hardware Implementation of Symmetric Algorithms for RFID Security", *RFID Security*.

Lehtonen, M., Ostojic, D., Ilic, A., Michahelles, F. (2009), "Securing RFID Systems by Detecting Tag Cloning", *Lecture Notes in Computer Science*, Vol. 5538.

Mitrokotsa, A., Rieback, M. R., Tanenbaum, A. S. (2009), "Classifying RFID attacks and defenses", *Information Systems Frontiers*.

Park, N., Song, Y., Won, D., Kim, H. (2008), "Multilateral Approaches to the Mobile RFID Security Problem Using Web Service", *Lecture Notes in Computer Science*, Vol. 4976.

Park, N., Won, D. (2008), "Dynamic Privacy Protection for Mobile RFID Service", *RFID Security*.

Sadeghi, A., Visconti, I., Wachsmann, C. (2009), "Location Privacy in RFID Applications", *Lecture Notes in Computer Science*, Vol. 5599.