RFID EPC-Gen2 for Postal Applications: A Security and Privacy Survey

Joan Melià-Seguí
Universitat Oberta de Catalunya
Rambla de Poblenou 156
08018, Barcelona - Spain
Email: melia@uoc.edu

Jordi Herrera-Joancomartí
Universitat Autonoma de Barcelona
Edifici Q, Campus de Bellaterra
08193, Bellaterra - Spain
Email: jherrera@deic.uab.es

Joaquin Garcia-Alfaro
Institut Telecom, Telecom Bretagne
02, rue de la Chatagneraie
Cesson-Sevigne 35576 - France
Email: joaquin.garcia-alfaro@acm.org

***Abstract*—Security and privacy on low-cost RFID deployments is focusing the attention of researchers due to the progressive adoption by retailers, making the RFID a real ubiquitous technology. Besides the retail sector, other logistics industries are starting to improve their processes with this technology like the postal companies, supposed to be one of the largest RFID sector. This paper is focused on the postal model of EPC RFID technology, and its security and privacy implications. We define a postal RFID threat context and propose measures to improve security and privacy in current RFID deployments.**

***Index Terms*—RFID, EPC, retail, logistics, postal, threat analysis, security, privacy.**

I. Introduction

LOW-COST Radio Frequency IDentification (RFID) tags are becoming a successful technology to increase the efficiency and productivity in the logistics sector. As the costs of tags are dropping, logistics departments are taking more attention to the possibility to integrate this real-time technology in the business processes in order to improve the visibility and accuracy of the logistic operations [1].

The deployment of the RFID technology is becoming more important thanks to the standardization process through the Electronic Product Code (EPC) Class 1 Generation 2 (hereinafter denoted as Gen2) tag standard [2] promoted by EPCglobal. EPCglobal standardization covers the whole RFID architecture, from tag data structure to network communication specifications. EPC tags are not provided of on-board batteries, but are passively powered through radio-frequency waves.

EPC tags have been seen by retailers as the perfect technology to increase the visibility of their products in the supply chain, improving in this way the efficiency of the logistic processes. Since Wal-Mart adopted this technology for its supplying processes and inventory control [3], other retail industry leaders have followed the same steps. Just as the EPC technology is beginning to be widely used in retail, there are other logistic industries introducing the benefits of the EPC inside different processes, like postal companies. Estimation for the RFID global market for the postal sector are optimistic [4]. When item level tagging (i.e. low-cost tagging like EPC) gains widespread acceptance, postal applications will be the second largest application of RFID in the world.

This work has been supported by the Spanish Ministry of Science and Innovation, the FEDER funds under the grants TSI2007-65406-C03-03 E-AEGIS, CONSOLIDER-INGENIO CSD2007-00004 ARES, an IN3-UOC doctoral fellowship, and the *future et ruptures* project LOCHNESS.

RFID technology brings potential benefits to the postal companies. Automatic non-assisted identification and product processing, global compatibility with standards and technology and reduction of expenses thanks to a major control over the logistic processes [4]. On the other hand, the EPC technology implies real disadvantages due to the limited computation resources of low-cost tags. EPC design was based on the idea to maximize the reduction of cost per tag (breaking the 5 cents frontier) to be more attractive for the industries. One of the most relevant problems related to this technology is the lack of security measures. Due to the insecure wireless channel, tags' information can be eavesdropped up to several meters, revealing the identification number (EPC) stored in the tag [5].

The main contribution of this paper is the specification of a postal RFID model, based on the retail RFID model along the supply chain, but focused on the postal applications singularities. This paper also contributes with a definition of security and privacy threats for postal RFID applications, regarding the insecure wireless channel in RFID technology. Finally a survey of implementable solutions for the specified threats is provided.

The remainder of this paper is organized as follows. In Section II we outline the methodology used to set up the postal RFID model. In Section III we overview the main threats of a postal EPC system. In Section IV we survey some security measures for the defined postal EPC model. We finally close the paper in Section V by summarizing the conclusions of our work, and looking to the future work perspectives.

II. Postal RFID model based on retail literature

RFID deployment is exponentially growing in the retail sector thanks to the adoption of EPC technology by supply chain industry leaders (like Wal-Mart or Metro). Retail industry is currently a developed scenario for RFID applications, and a reference for future RFID implementations in other sectors. Different proposals for models and examples of EPC implementations in retail can be found in the literature [6], [7]. In this section, we review the main properties of the retail environment in order to define a postal model. Such identification allows us to analyze the security of the postal

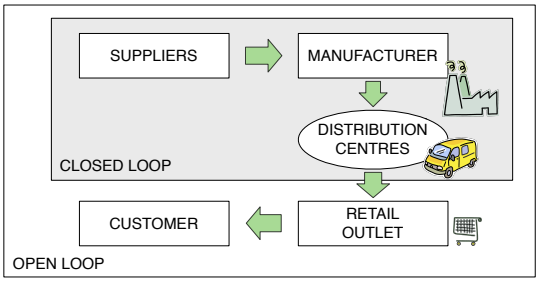

Fig. 1. Retail RFID model.

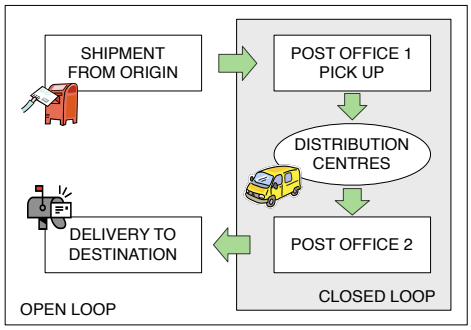

Fig. 2. Postal RFID model.

model in a similar way as it has been done for the retail environment.

Detailed in the standard [8], a simplified EPC based system in a company A can be defined as a set of the following elements: a set T_A of tags and a set R_A of readers connected to a middleware M_A and other information systems IS_A. Moreover, if the information needs to be accessible outside of this domain (company A) then an Object Name Service (ONS) must be enabled.

A. Retail model

Wal-Mart was the first big company requiring to all suppliers to attach an EPC label to all the pallets and cases shipped to the retailer's distribution centers and stores [3]. Another retail pilot was launched by Metro Group's Galeria Kaufhof, being the world's first end-to-end EPC item-level application [6]. In a resumed way, the process begins at the manufacturing process of a company A, when a tag $t \in T_A$ is attached to the good, and finishes at customer property (giving the option to remove the tag at point of sales). The proliferation of companies adopting RFID for their logistic processes caused the definition of a formal model for the RFID application in the retail industry (e.g. [7]). The specific steps in the retail RFID model can be summarized in the following four stages (cf. Figure 1).

- Manufacturing (including suppliers)
- Distribution Center (logistics delivery)
- Retail outlet
- Customer

The retail model cited in this section can be classified inside the *open-loop* class, described in [9]. An *open-loop* RFID system assumes that tagged items do not come back to their originator at all or if so, for a long period of time or for end-of-life processes (end-to-end processes). Tagged objects are usually individual items, which are permanently associated and identified for life-cycle management or track and trace applications.

On the other hand there are also *closed-loop* RFID systems. This case supports a very specific set of processes where items equipped with RFID tags are used or reused among a predetermined group of partners. Typical use cases include the tracking of reusable assets between manufacturer and specific suppliers. Tagged objects are usually reusable assets such as trolleys or pallets that continuously come back to their originator [10].

B. Postal model

According to this retail model, we define a postal model by considering current EPC RFID pilot projects developed by postal companies in Korea, China, Kingdom of Saudi Arabia (KSA) and Spain.

The Electronic and Telecommunications Research Institute (ETRI) has developed a postal RFID system proposal, including possible RFID applications for postal management [11], [12]. The proposal contains specifications for parcel process and pallet management. It also includes an RFID tag data structure for postal process, and a real-time monitoring application. Statistics management of parcel processing and pallet usage, are also included in this RFID project proposal.

Beyond system proposals, some postal companies have taken the first step deploying different applications with RFID systems. This is the case of the Spanish Post Company who has provided to all its distribution centers (DC) with an EPC system to track quality of service (QoS) measurements [13]. The system works as follows; selected users inside the quality program crosses tagged letters t_Q to other users or post offices, traveling across different regions. Each region is managed by a DC where an EPC control system is implemented (readers and antennas R_Q), sending the relevant information to the quality application (back-end system composed by a middleware software M_Q)and an information system IS_Q to connect to central server). This process is constantly repeated by over five thousand tagged letters, obtaining a real on-line time-delivering map.

Following the idea of the end-to-end RFID applications, Saudi Post is installing individual mail boxes equipped with an EPC tag (e-boxes) for QoS improvement and postman performance control [14]. Saudi's project, like Spain's Post and the ETRI proposal, can be classified into *open-loop* applications following a similar end-to-end scheme.

Figure 2 summarizes the different steps of the referred postal RFID projects, defining a generic postal RFID model that can be applied to other postal applications. Each postal step definition represents an RFID tracking point:

- Shipment from origin: A tagged letter $t \in T_P$ is sent from origin to any destination. Postmen can be equipped with a hand-held RFID reader R_P or an embedded system in the mail-trolley or car, to release the first RFID trace. Also mailboxes can be provided with RFID identification (tagged mailboxes or embedded RFID reader).
- Post office 1 / Pick up: Reception Post Office is the first step where letters are recognized and distributed (local shipments are delivered without passing through any additional step). Depending on the product, the sender can go directly to the Post Office where the parcel or letter is tagged in the pick up process, thus bypassing the previous step.
- Distribution Centers: DC's network distributes the postal traffic from / to its own regions. Each DC is provided with an RFID control system R_P, thus the tag ID, the exact day, time, and the dock-door where the truck is loading or unloading the mail, is automatically registered by the RFID application M_P.
- Post office 2: Reception Post Office receives classified mail ready to be delivered by the postmen.
- Delivery to destination: Postman delivers mail to all destinations. This is the last opportunity for the postal company to track the mail by using hand-held RFID readers R_P. Also personal mailboxes can be provided with RFID identification (tagged mailbox or embedded RFID reader).

Besides the model described above, we can also find *closed-loop* postal applications where the objects to track are not the letters (delivered and received by users), but the logistic infrastructure used by the company to distribute the products (e.g. letters or parcels) inside the company facilities. This is the case of China's Post mailbags management [15] and the Spain's Post containers management [13]. However, as we will see in the security analysis (cf. Section III), the *closed-loop* model is less susceptible to security threats than *open-loop* because it is developed in controlled environments.

Before introducing the security analysis, it is important to notice the main difference between the retail and postal model regarding the RFID scenario. The start point of the retail model, the suppliers and manufacturing process, is performed inside the company facilities. That means all operations (including RFID operations such as labeling or identification code writing) are performed in a controlled environment, where physical security measures like personal access control are operative. The first point where customers have access to the RFID tagged products is the retail outlet, in the border of *closed loop* and *open loop* model (cf. Fig. 1). On the contrary, the start point for the postal model is outside the *closed loop*, meaning that tagged letters or parcels are accessible to everyone, thus counterfeited products can access the classification and distribution processes (cf. Fig. 2). To sum up, the *closed* and *open loop* configuration of the retail and postal model raises a significant difference regarding the logistics process and its RFID application. Although the final step is equivalent for both retail and postal models, the beginning is totally different, thus both models must be analyzed independently regarding all the issues, e.g. security and privacy.

III. Threats in Postal RFID model

Like any other information system model, the EPC architecture may suffer threats regarding the privacy and security of the information managed by the system, even more if the communications channel is highly insecure [16], because the confidentiality of the transmitted data between readers and tags is not guaranteed. Regarding this scenario, most of the security and privacy threats on EPC based systems will target the wireless interface [17]. This paper is focused on the main threats regarding the lack of authentication and security measures of EPC tags [18] and the insecure wireless communication channel between tags and readers [19], thus a secured system from reader to middleware and above (wired network) is assumed. Analysis in other security domains can be consulted in [17].

Back to postal RFID model, we define known threats for the postal EPC system (defined in Section II) based on the retail experience. In [20] the authors have defined three major contexts for EPC tags based on the retail sector namely: *Inside the supply chain*, *the transition zone* and *outside the supply chain*. In Table I we define the mentioned context based on the postal model and the kind of application-loop. Security and privacy threats in EPC systems regarding the retail model, have been analyzed by different authors (e.g. [21], [16], [20]). The following, are active and passive [22] threats applying the postal RFID model:

- Spoofing: Threat where an attacker falsifies its identity (or its resources) with that of a legitimate system user, with the aim to infringing authentication. In the case of RFID, an illegitimate reader inside the postal process, could spoof a legitimate one, obtaining information from the system in a fraudulent way. Since the EPC system does not have authentication mechanism, the attacker will not find any difficulty to obtain the same information than a legitimate user. This threat is specially relevant because the information stored in the EPC code can reveal sensible information about the user, the client code, the postal code or the shipment value, as well as the postal company strategies [17]. An example of this threat is a Man-in-the-Middle (MitM) attack.
- Counterfeiting: Seeks to undermine the integrity of an object, in the case of RFID, modifying the information stored in the tag memory $t \in T_A$. Counterfeiting the stored data in an EPC tag, product tampering could be achieved in the postal process itself. Cloning a tag ID is an example of this threat.
- Denial of Service (DoS): Threat where an attacker has the aim to limit the availability of th service. For example, an attacker can use an RFID reader to transmit signal jamming in order to disable the RF channels, or even killing the tag with the killing option provided by the standard [2].

TABLE I
POSTAL RFID THREATS CONTEXT.

Context	Postal	Model	Application
Inside the supply chain	Includes all DC's, as well as transportation systems and others post office's classification areas.	DC's	Open-loop & closed-loop
The transition zone	The post office area where tagged mail is delivered to / from the customer	Post office 1	Open-loop & closed-loop
		Post office 2	
Outside the supply chain	Including all external locations, especially mailboxes.	Shipment from origin	Open-loop
		Delivery to destination	

- Eavesdropping / Information disclosure: As said in previous sections, communication channel between readers R_A and tags T_A is accessible due to the insecure wireless channel, thus the confidentiality of the service is easily vulnerable. Illegitimate scanning of this communication can be done just by using a compatible reader. This threat is specially relevant due to the signal power transmitted by the EPC readers, which can be received up to hundreds of meters [2]. Personal privacy threats like tracking or profiling / clustering analysis are included in this category [20].

On the other hand, mailboxes or even tagged letters can suffer physical attacks such as tag removing, deactivation or replacing by a new one. This threat is only possible in non controlled contexts like outside the *closed loop*, where the shipment and delivery to destination processes are done. This threat is not included in the analysis because a physical action is required, thus alternative solutions outside the field of this paper are necessary to solve this threat.

Figure 3 shows a contextualization of known threats for retail to the postal model, based on threats-context analysis of [20] and the postal model defined in Section II. We have highlighted the specific threats that apply to the postal model that where not present in the retail model.

Threats to the RFID infrastructure of the postal model are not only relevant for the information security itself, but for the economic value associated to it. Regarding the Universal Postal Union sources, over three billion US dollar will be spent in the next few years on acquiring RFID equipment by postal companies [4]. Besides the RFID infrastructure, RFID tagged postal processes are also economically relevant. China Post processes over a million postal bag containers daily [23]. Also about 6 million post boxes with an RFID tag (with personal information such as the address) have been installed in the United Kingdom [4]. The threats associated to the RFID postal model, and therefore its economic impact, make necessary the adoption of security and privacy measures to reduce the motivation of possible attacks.

IV. SECURITY MEASURES FOR POSTAL RFID MODEL

RFID postal applications are in an early stage compared to retail applications. However RFID postal applications are being developed at the moment in both *closed* and *open-loop* scenario [13], but as far as we know there is not any security analysis for postal sector applications.

Focusing on the context-threat analysis defined in Section III, *open-loop* postal service is more exposed to privacy and security risks since tags are outside a controllable environment both at the beginning and at the end of the application. As shown in Figure 3, the user to post office and vice versa are the steps outside the DCs and in the post offices (transition zone), thus the more risky steps from the privacy point of view.

Low-cost RFID security related literature, brings security improvement solutions by modifying the communication protocols [24] or the chip capabilities of the EPC Gen2 standard [25]. The implementation of these proposals is not feasible in current EPC installations because the chip modifications are not compatible with the EPC Gen2 standard. Even solutions requesting a number of logical gates available in the current chip, are not possible to implement in current deployments because a modification of the standard must be done before.

In the following paragraphs we survey a set of current and proposed solutions for an EPC postal model. These proposals are implementable in current installations because it does not require the implementation of the standard. In order to analyze the suitability of this measures, we will use the postal scenario defined in Section II, and specifically the threat context of Table I and Figure 3.

A. Analysis of security measures implemented in EPC tags

EPCglobal provides an on-board security option known as *kill command* [2]. Enabled with a 32 bits password, this command disables the tag performance permanently. This utility solves threats like eavesdropping but eliminates any option of post-shipment service for the customer. Due to the postal RFID model uniqueness, tags will be exposed to threats at the beginning of the shipment (cf. Figure 3), thus killing is not a suitable measure for security and privacy improvement in a postal environment.

Furthermore the standard also includes a 32 bits *access password* [2]. With the access password on, the writing on tag option is blocked. This measure can solve threats like *counterfeiting* if the attacker does not know the password, but the rest of threats are still open.

B. Implementable solutions at high level

The following approaches to RFID security and user privacy measures have been proposed in the literature to be implemented in the EPC Information Services (IS_A) or Middleware (M_A), thus suitable to the proposed EPC postal model.

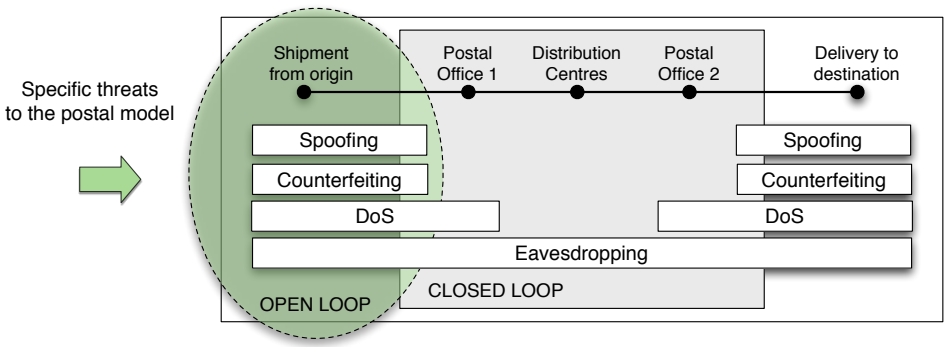

Fig. 3. Proposed threat model for postal EPC model.

- ID rewrite or encryption is the concept for measures like *ID relabeling* [26], [27], [28]. In a resumed way this measures take advantage of the rewriting possibility of the tag to avoid threats like *eavesdropping* or *spoofing*. Both relabeling and ID encryption responds to the same idea: link in a secured database the real tag ID and a *pseudo ID* that can be a simple pseudonym or an encryption of the valid ID.
  Once the pseudonym is computed, it is write in the tag ID memory. Both pseudonym and real ID are stored in a secured database to be accessible by the system. This measure does not solve a possible *counterfeiting* attack at the end of the postal chain, or in contexts where tags are not rewritten. *DoS* is not solved by this measure, because tags will loose all its performance properties.

- Physical protection of tags can also be used for security and privacy purposes. Shielding of tags (e.g. metallic bag) is proposed in [21] to avoid the activation of the tag response. Also printing on the letter or parcel the ID codified in a barcode or similar, can be understood as a backup of the legitimate ID, avoiding possible *spoofing* or *counterfeiting* threats, as well as *DoS*.

- Active jamming of RF signals is cited in [21]. By using a RF transmitter occupying all the RFID channels (a kind of intentioned *DoS*), actions like *eavesdropping* or *spoofing* can be avoided in the vicinity. Applying this measure means no traceability in the active jamming environment, thus implementations like the proposed in [11] could not be carried out. *Counterfeiting* threat is not solved by this measure considering that active jamming cannot be done everywhere. Similar to this, the Blocker Tag proposal [29] can also avoid illegitimate access to the RFID identification.

- Trusted Tag Relation is based on the idea of a trusted steps configuration. Following the concept of [30] a tag $t \in T_A$ is validated by an authorized party in the beginning of the postal process (e.g. the postal company A) by scanning the letter with a hand-held RFID reader R_A connected to the information systems IS_A, and marking the status of *valid*. The following steps will trust on t information only if the step-before has validated the integrity of the information stored in t. This measure helps to identify more easily *counterfeiting* actions, but is not suitable for *eavesdropping* or *spoofing* actions because t_{ID} is not modified in all the process. Neither solves *DoS* scenarios because readers cannot work correctly.
  Another security-distributed approach is the secret-sharing scheme with distributed keys proposed in [31]. A distributed key k is used to encrypt the tag ID, but it is distributed among several readers. To recover the ID of the tag, information obtained from all the readers is necessary.

- ID with message authentication code (MAC) is to concatenate a reduced ID, with an ID authentication code, with the aim to improve the integrity of the information stored in the tag. If we only use 50 bits of information (equivalent to more than a million combinations for each habitant in Spain) to manage the tag ID in the postal chain, the remaining 46 bits (for the EPC Gen2) can be used to protect the main ID content, and detect possible *counterfeiting* threats. The utilization of a *hash* function with a key k (only known by the postal company) can be a useful option to obtain the authentication code. In this way, the final ID (96 bits) would be the result of concatenating the original ID, with the result of applying a *hash* function with key k to the *XOR* sum of k and ID_{50bits}:

$$ID_{96bits} = ID_{50bits} | H_k(ID_{50bits} \oplus k)_{46bits}$$

  The operation would be done in IS_A or in R_A, and the result would be written in the tag ID memory. It is important to stand out that a *brute force attack* will eventually reveal k. Using a great diversity of passwords (e.g. according to the postal product, postal code, destination city, data of shipment) can improve the data integrity in the system.

V. Conclusion

The massive incorporation of RFID technologies in retail logistics has motivated the study of threats against their security and privacy. Weak points have been identified and addressed in the literature. The optimistic prevision of the RFID adoption by the postal sector, opens a new field for similar analyses based on the postal model uniqueness.

In this paper, the authors have analyzed the current RFID postal implementations based on EPC technology, defining a RFID postal model proposal based on the existing scientific literature and real implementations. Furthermore we have translated the existing security and privacy analysis for the retail sector to the proposed postal model obtaining four major threats: eavesdropping, DoS, counterfeiting and spoofing. We have also identified the specific threats applying the postal RFID model, and we have detailed the security issues ragarding the open and closed loop model differences.

Current measures are focused on solving specific threats (passive attacks like eavesdropping or spoofing actions) but only measures regarding *ID relabeling* or *encryption* can be applied in some cases due to the uniqueness of the postal model. Furthermore we survey security measures to detect counterfeiting threats related to the postal model, or even recovery the tag's information in *DoS* situations.

Future research lines will focus into identifying specific security problems in the postal model edges, where the system is more vulnerable.

References

[1] Motorola, "RFID technology and EPC in retail," Whithe Papers, (last access feb. 2010). [Online]. Available: http://www.motorola.com/rfid/

[2] EPCglobal, "EPC radio-frequency identity protocols class-1 generation-2 UHF RFID protocol for communications at 860-960 MHz," Tech. Rep., 2007. [Online]. Available: http://www.epcglobalinc.org/standards/

[3] RFID Journal, "Wal-mart opts for EPC class 1 v2," Tech. Rep., (last access feb. 2010). [Online]. Available: http://www.rfidjournal.com/article/articleprint/641/-1/1/

[4] Universal Postal Union, "A market hungry for chips," Tech. Rep., (last access feb. 2010). [Online]. Available: http://www.upu.int/union_postale/2007/en/3-4.html

[5] K. Deeb, "Efficiency, privacy and security analysis of ubiquitous systems in the retail industry," *Innovations in Information Technology*, pp. 1–6, nov. 2006.

[6] RFID Journal, "Metro group's galeria kaufhof launches UHF item-level pilot," Tech. Rep., (last access feb. 2010). [Online]. Available: http://www.rfidjournal.com/article/articleprint/3624/-1/1/

[7] G. Roussos, "Enabling RFID in retail," *Computer, IEEE*, vol. 39, no. 3, pp. 25–30, mar. 2006.

[8] EPCglobal, "The EPCglobal architecture framework," Tech. Rep., 2007. [Online]. Available: http://www.epcglobalinc.org/standards/

[9] P. Schmitt, F. Michahelles, and E. Fleisch, *An adoption Strategy for an Open RFID Standard, Withe Paper - Business Processes & Applications*, 1st ed., Auto-ID Labs, sep. 2005, (last access feb. 2010). [Online]. Available: http://www.autoidlabs.com

[10] E. Flelsch, J. Ringbeck, S. Stroh, C. Plenge, L. Dittmann, and M. Strassner, *RFID - The Opportunity for Logistics Service Providers, Withe Paper Series*, 1st ed., Auto-ID Labs, sep. 2005, (last access feb. 2010). [Online]. Available: http://www.autoidlabs.com

[11] J.-H. Park, J.-H. Park, and B.-H. Lee, "RFID application system for postal logistics," *Management of Engineering and Technology, Portland International Center for*, pp. 2345–2352, aug. 2007.

[12] Y. Choi, J. Won, and J. Park, "An experimental testbed for parcel handling with RFID technology," *Advanced Communication Technolgoy - ICACT*, vol. 1, no. 20-22, pp. 321–326, feb. 2006.

[13] RFID Journal, "Spain's post office improves delivery speed," Tech. Rep., (last access feb. 2010). [Online]. Available: http://www.rfidjournal.com/article/articleprint/3209/-1/1/

[14] M. B. Anzzan. (2007, oct.) Saudi post RFID implementations. Saudi Post. Postal Technology Workshop (Beijing - China). [Online]. Available: http://www.upu.int/info_tech/en/2007-10-16_workshop.shtml

[15] RFID Journal, "China post deploys EPC RFID system to track mailbags," Tech. Rep., (last access feb. 2010). [Online]. Available: http://www.rfidjournal.com/article/articleprint/2487/-1/1/

[16] S. Weis, S. Sarma, R. Rivest, and D. Engels, "Security and privacy aspects of low-cost radio frequency identification systems," in *International Conference on Security in Pervasive Computing – SPC 2003*, ser. LNCS, D. Hutter, G. Müller, W. Stephan, and M. Ullmann, Eds., vol. 2802. Boppard, Germany: Springer-Verlag, mar. 2003, pp. 454–469.

[17] J. Garcia-Alfaro, M. Barbeau, and E. Kranakis, "Analysis of threats to the security of EPC networks," *Sixth Annual Communication Networks and Services Research (CNSR) Conference, Halifax, Nova Scotia, Canada*, may. 2008.

[18] D. R. Thomson, N. Chaudhry, and C. W. Thompson, "RFID security threat model," *Conference on Applied Research in Information Technology*, 2006.

[19] D. C. Ranasinghe and P. H. Cole, "Confronting security and privacy threats in modern RFID systems," *Signals, Systems and Computers, 2006. ACSSC '06. Fortieth Asilomar Conference on*, pp. 2058–2064, oct. 2006.

[20] S. Garfinkel, A. Juels, and R. Pappu, "RFID privacy: An overview of problems and proposed solutions," *IEEE Security & Privacy IEEE*, vol. 3, no. 3, pp. 34–43, jun. 2005.

[21] P. Peris-Lopez, J. C. Hernandez-Castro, J. Estevez-Tapiador, and A. Ribagorda, "RFID systems: A survey on security threats and proposed solutions," in *11th IFIP International Conference on Personal Wireless Communications*, ser. LNCS, vol. 4217. Springer-Verlag, sep. 2006, pp. 159–170.

[22] L. Buttyan and J.-P. Hubaux, *Security and Cooperation in Wireless Networks*. Cambridge University Press, 2007.

[23] RFID Group of China Post. (2007, oct.) QoS measurement system for mail flows. China Post. Postal Technology Workshop (Beijing - China). [Online]. Available: http://www.upu.int/info_tech/en/2007-10-16_workshop.shtml

[24] M. Lehtonen, T. Staake, F. Michahelles, and E. Fleisch, "From identification to authentication - a review of RFID product authentication techniques," Printed handout of Workshop on RFID Security – RFIDSec 06, Ecrypt, Graz, Austria, jul. 2006.

[25] M. Feldhofer, J. Wolkerstorfer, and V. Rijmen, "Aes implementation on a grain of sand," *IEE Proceedings - Information Security*, vol. 152, no. 1, pp. 13–20, 2005.

[26] A. Juels, "RFID security and privacy: A research survey," *IEEE Journal on Selected Areas in Communication*, vol. 24, no. 2, pp. 381–394, feb. 2006.

[27] K. H. Wong, P. C. Hui, and A. C. Chan, "Cryptography and authentication on RFID passive tags for apparel products," *Computers in Industry*, vol. 57, no. 4, pp. 342–349, may. 2006.

[28] S. Weis, S. Sarma, and D. Engels, "RFID systems and security and privacy implications," in *Cryptographic Hardware and Embedded Systems – CHES 2002*, ser. LNCS, B. Kaliski, c. Kaya ço, and C. Paar, Eds., vol. 2523. Springer-Verlag, aug. 2002, pp. 454–469.

[29] A. Juels, R. L. Rivest, and M. Szydlo, "The blocker tag: selective blocking of RFID tags for consumer privacy," in *CCS '03: Proceedings of the 10th ACM conference on Computer and communications security*. New York, NY, USA: ACM, 2003, pp. 103–111.

[30] A. Solanas, J. Domingo-Ferrer, A. Martínez-Ballesté, and V. Daza, "A distributed architecture for scalable private RFID tag identification," *Computer Networks, Elsevier*, vol. 51, no. 9, jan. 2007.

[31] A. Juels, R. Pappu, and B. Parno, "Unidirectional key distribution across time and space with applications to rfid security," in *SS'08: Proceedings of the 17th conference on Security symposium*. Berkeley, CA, USA: USENIX Association, 2008, pp. 75–90.