Title	**Data Management ofRFID-based Track-and-Trace Anti-counterfeiting in Apparel Supply Chain**
Author(s)	**Choi, SH; Yang, B; Cheung, HH; Yang, Y**
Citation	**The 8th International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 9-12 December 2013. In International Conference for Internet Technology and Secured Transactions Proceedings, 2013, p. 265-269**
Issued Date	**2013**
URL	**http://hdl.handle.net/10722/198612**
Rights	**International Conference for Internet Technology and Secured Transactions Proceedings. Copyright © I E E E.**

Data Management of RFID-based Track-and-Trace Anti-counterfeiting in Apparel Supply Chain

S.H. Choi, B. Yang, H.H. Cheung, and Y.X. Yang
Department of Industrial and Manufacturing Systems Engineering,
The University of Hong Kong, Pokfulam Road, Hong Kong
shchoi@hku.hk, {yangboo2009, hhoicheung, tinayang54}@gmail.com

***Abstract*—With recent advancement in Radio Frequency Identification (RFID), RFID-based track-and-trace anti-counterfeiting has attracted considerable research interests. A track-and-trace anti-counterfeiting system requires an integral and reliable electronic pedigree (e-pedigree) to ensure high product visibility along the supply chain. With the continuous movements of large volumes of products along the supply chain, huge amounts of RFID data would be inevitably generated, posing great challenges to system development and operation. As such, the front-end RFID data should be well-formatted for efficient capturing, filtering, and synchronization in a logical and reliable way, so that the accumulated e-pedigree would be complete and trustworthy for subsequent product authentication. In this paper, we present an innovative track-and-trace anti-counterfeiting system for apparel products, and discuss a number of key data management issues, such as e-pedigree formatting, data synchronization, and traceability / visibility control. A data format of e-pedigree for full traceability of garments is proposed to support products authentication in item-level, products anti-lost in pallet-level and products status prediction in batch-level. Based on this format, a three-step mechanism of data synchronization is established to ensure e-pedigree integrity. To avoid possible leakage/falsification of e-pedigree data, an RBAC-based access control is proposed as an auxiliary module of the anti-counterfeiting system.**

Keywords-RFID, track-and-trace, anti-counterfeiting, data management, e-pedigree formatting/synchronization.

I. INTRODUCTION

Product counterfeiting is an illicit practice of copying a genuine item and creating a fake version. It poses huge threats to the manufacturing industries and the global economy. The number of counterfeit products has been skyrocketing in recent years. The International Anti-Counterfeiting Coalition (IACC) [1] estimates that $600 billion is lost annually due to counterfeiting. This has called for a reliable anti-counterfeiting technology to safeguard authentic products, to help companies fight illicit competition, and to protect the interest of end-consumers.

Current anti-counterfeit technologies can be broadly categorized as follows: 1) Overt, or visible features; 2) Covert, or hidden markers; 3) Forensic techniques; 4) Serialization/Track-and-Trace systems. The principles and detailed comparisons of these anti-counterfeiting approaches are elaborated in [2][3][4][5]. Among them, the track-and-trace approach is found outstanding in combating counterfeiting. In particular, the track-and-trace approach is distinguished by its ability to protect the whole supply chain against infiltration and abuse, as well as the additional benefits in enhancing the supply chain efficiencies, eliminating theft and fraud, facilitating recall of defective products and remote authentication.

Track-and-trace anti-counterfeiting may be based on barcodes (linear or 2D matrix) or RFID tags for identification of product items. An RFID tag comprises of an antenna within a microchip, which contains specific item-level product information. The information can be interrogated at a certain distance by RFID readers through electromagnetic waves. Compared with barcode, RFID-based system tends to be much more advantageous, in that it is capable of automatically identifying/authenticating products with non-line-sight, and that it supports fast and massive reading.

With the increasing popularity of RFID in supply chain management during the past decade, a number of RFID-based traceability systems have been established in [6][7][8][9]. However, these systems tend to target at some specific applications of supply chain management, such as inventory control, eliminating wastage, and fine grain product recalls. The concept of utilizing RFID tags to track-and-trace products for anti-counterfeiting through the whole supply chain was first proposed in [10] and analyzed in [11][12][13][14]. With the evolvement of RFID technology and maturity of item-level applications, some researchers have proposed detailed system architectures [10][15][16] to combat counterfeiting. However, few have been implemented in practice. Indeed, there still exist a number of practical issues which have yet to be solved, especially the issues of data management.

As RFID-tagged product items flow along the supply chain, the track-and-trace anti-counterfeiting system dynamically generate a large amount of data about product state changes [17], which form the skeleton of the product e-pedigree stored in the databases at the back-end servers. Considering the great importance of e-pedigree for anti-counterfeiting, three key issues, namely Pedigree Data Formatting, Pedigree Data Processing and Pedigree Transmission Mechanism, have to be addressed accordingly [18].

Pedigree Data Formatting is essential for collection and management of data in an expressive format that facilitates product ID generation, item tracking, authenticating and monitoring. Pedigree Data Processing refers to the procedure or

978-1-908320-20/9/$25.00©2013 IEEE

mechanism used to update/synchronize e-pedigree data to keep its integrity. Indeed, the reliability of a track-and-trace anti-counterfeiting system hinges largely on the e-pedigree data formatting and synchronization. Pedigree Transmission Mechanism is a mechanism for controlling access to the pedigree data, as required for internal/legal/government audit. In fact, this issue calls for a proper data visibility mechanism to deal with several possible high-level scenarios, such as government inspection and after sale processing. These scenarios involve human interactions with the anti-counterfeiting system and thus should be well-controlled to avoid data leakage/falsification or corrupting the entire system. Overall, irrespective of the detailed architecture of a track-and-trace anti-counterfeiting system, the data management issues of e-pedigree, such as data formatting and synchronization, have to be fully addressed.

This paper therefore attempts to deal with these issues. We focus on designing an e-pedigree data structure and format for apparel products, and on establishing a data synchronization mechanism for maintaining e-pedigree integrity and controlling data visibility for human (internal employee/government) interaction. We first present an innovative RFID-aided track-and-trace anti-counterfeiting system in section 2. Based on this system architecture, the design of a data format for e-pedigree of apparel products is proposed in section 3. An automatic data synchronization mechanism is then elaborated in section 4, while control of data visibility is explored in section 5. Lastly, a conclusion is drawn and future work discussed in section 6.

II. A PROPOSED RFID-BASED TRACK-AND-TRACE ANTI-COUNTERFEITING SYSTEM

Based on our previous work [15], we proposed an RFID-based track-and-trace anti-counterfeiting system for relatively high-end products. The system architecture is shown as in Fig 1. It mainly consists of two layers, namely a front-end RFID-enabled layer for tag programming and product data acquisition, and a back-end anti-counterfeiting layer for processing and synchronization of product e-pedigree and authentication.

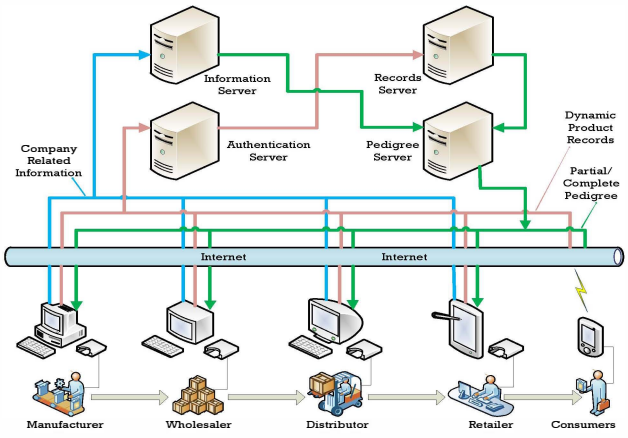

Figure 1. An RFID-based Track-and-Trace System Architecture

The back-end layer consists of a set of computer servers which together enforce track-and-trace anti-counterfeiting. The Information Server collects company related information from the supply chain partners through a system registration module. The information is crucial for the product pedigree because they form the basic geographical picture of the product movement history in supply chain; it also provides the basis for tracing problems when suspected counterfeits emerge. Each product is identified by an embedded RFID tag, which is programmed with a unique product identifier (PID). The PID forms the basis of a transaction record, which is sent to the Authentication Server. The Authentication Server verifies the transaction records and screens out suspicious activities. The screened records are then sent to the Record Server for storage and subsequent follow-up. The supply chain partners can verify the partial product pedigree from the point of manufacturing to the previous owners by making requests to the Pedigree Server, which in turn retrieves transaction records from the Records Server as well as company information from the Information Server to generate the required pedigree. They should reject any products with a suspicious partial pedigree. The Pedigree Server is also responsible for generating complete product pedigrees, through the Internet and the mobile phone network, to end-consumers for verification. When a customer is satisfied that a product is genuine and has paid for it, the retailer should generate a sale record, which is subsequently sent to the Authentication Server. Any further transactions of the same product after the sale record are deemed suspicious.

The front-end layer mainly controls RFID devices to read (program) data from (to) the tags attached to product items for processing the data together with the related product information. This layer is particularly crucial to establishing and ensuring accurate e-pedigrees that record all transactions of each of the product items moving along the supply chain, from the manufacturing source to the retail stores.

III. FORMATTING E-PEDIGREE DATA FOR APPAREL PRODUCTS

Based on the proposed system architecture for RFID-enabled track-and-trace anti-counterfeiting described in section 2, we now outline the issue of e-pedigree data formatting and then propose a structure to standardize apparel product e-pedigree information.

In apparel supply chain, each garment is associated with an RFID tag which owns a PID generated during manufacturing. This PID serves as a pointer to the e-pedigree data subsequently accumulated in back-end databases. Apparently, full traceability of product items warrants some rules for data collection and transfer at each node of the supply chain. These data should be standardized and concise but comprehensible such that the accumulated e-pedigree is informative and convincing for product authentication. Otherwise, the whole concept of track-and-trace anti-counterfeiting would collapse. Several workgroups are reportedly developing methodologies of data standardization for applications like food track-and-trace check in the EU and can-trace data standard in Canada [19]. In the following section, we propose a structure to model apparel product e-pedigree data according to the proposed system architecture.

A convincing e-pedigree structure that facilitates full traceability of a product requires information of its total

lifecycle. This information can be mainly divided into three categories according to the four-element structure for traceability: (1) static data on logistics units; (2) static data on individual item features (PID); and (3) dynamic data on product state changes (e.g. transaction records) [18].

As mentioned in section 2, static data of logistics units includes all the information of the related supply chain companies which lays the foundation of the product e-pedigree. The PID of a product item simply contains the product feature information, which serves as a pointer to the accumulated e-pedigree data. Dynamic product data consists of item-level release records, transaction records, sale records, pallet-level containment relationship records, and batch-level order information. An indicative categorization of e-pedigree data for apparel products is summarized in Table 1.

TABLE I. E-PEDIGREE DATA FOR APPAREL PRODUCTS

E-pedigree Data Structure	Data Field	Description
Company Related Data	company name	A logistics unit in the apparel supply chain.
	company type	The type may be manufacturer, wholesaler, retailer, etc.
	address	It is crucial to form a geographical map for product movement in the apparel supply chain.
	status	Indicates the validation of the company.
	contact person	For management use.
Unique PID (RFID tag)	TID	Contains the UID of a tag, which is factory-locked and difficult to clone.
	EPC	Information about garment colour, size, etc.
Dynamic Product Records	release record	Includes the PID of a product item, companies involved, time of record, etc. (for manufacturers use)
	transaction record	Includes the PID of a product item, companies involved, time of transaction, etc.
	sale record	Includes the PID of a product item, companies involved, sale time, etc. (for retailers use)
	containment relationship records	Include relationship between items and cases, cases and pallets, etc.
	order records	Serve as advanced shipping notes for tracking of product status.
	mark fake records	Serve as a black list recording suspicious items detected by the system.

The proposed e-pedigree data structure is designed to support full product track-and-trace in apparel supply chain for anti-counterfeiting. It can be rearranged into three parts, namely PID, Trace Data, and Track Data, as shown in Fig 2. Item PID serves as a pointer that points to historical data (company information, records, containment relationship, etc.) and future state (downstream company information).

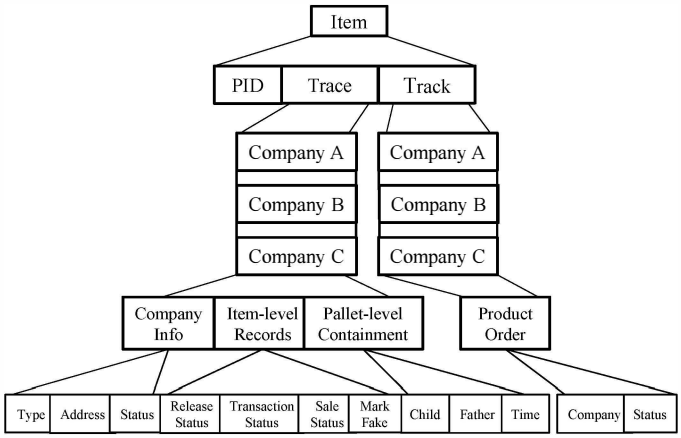

Figure 2. Data Structure of Apparel Product E-pedigree

Compared with the current track-and-trace systems [6][8][10][16], this e-pedigree data format is characterized by (1) integrity of physical companies; (2) item-level-enabled tracking/authentication; (3) support of pallet/case-level tracking and anti-theft/anti-lost; (4) support of batch-level order tracking and product status prediction.

IV. AN AUTOMATIC MECHANISM FOR DATA SYNCHRONIZATION OF E-PEDIGREE

As mentioned earlier, the track-and-trace method for anti-counterfeiting hinges on reliable data updating and synchronization between the front-end supply chain partners and the back-end databases, such that the data for physical movement of all product items are recorded in the e-pedigree. However, without an effective mechanism with proper logics for this purpose, the product e-pedigree can be deemed incomplete and dubious. As a result, fake injection cannot be effectively prevented, and the authenticity of a product item becomes unconvincing even if it has a genuine release record from the factory line.

In our proposed RFID-based track-and-trace anti-counterfeiting system, the back-end servers individually or cooperatively process data updating and synchronization. In general, it can be categorized into three steps to update and synchronize all the e-pedigree data through Information Server, Authentication Server and Pedigree Server, namely Company Registration, Product Release Updating and Product Transaction Recording.

When a supply chain company (a manufacturer, distributor, carrier or retailer) joins in the proposed RFID-aided traceability system, it should first access a registration module which captures the company information, such as company type, address, status and contact person. It should be noted that the company address is essential to forming a geographical map for product movement in future. The status is set as Pending by default; only after the System Holder (usually a Corporation Head or an entrusted third-part entity) checking the validation of the registered company, the status would change to Active, which symbolizes the success of company registration. After this, the registered company is assigned a unique ID and its contact person is able to add more peers and access the system to process front-end tagged apparel products, which goes to the

second step. Company Registration is mainly processed by Information Server, as shown in the Fig 3.

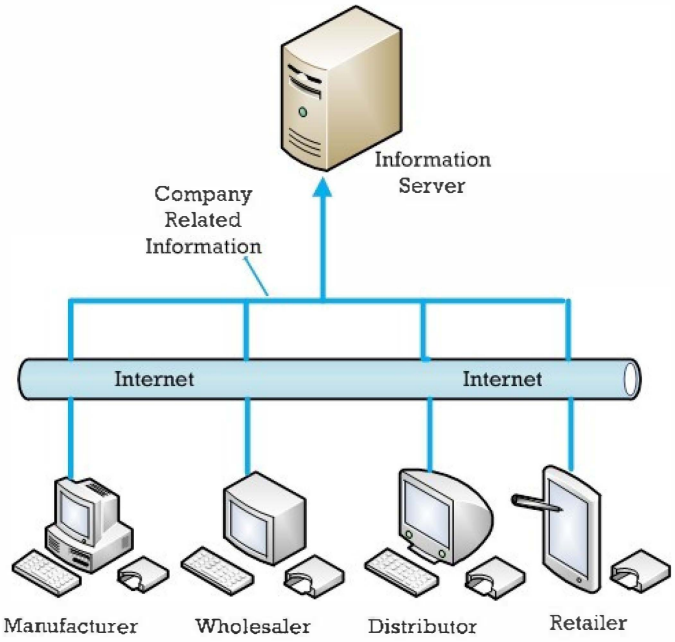

Figure 3. Company Registration

The second step of data synchronization is tailored for manufacturers to update product release information. In the front-end factory lines, an Active manufacturer is firstly required to access the system before production, getting the right to write item Release Records. When a product item finishes production (including real-time RFID tag programming of PID), a Release Record is composed and then updated to the Authentication Server for storage. It should be noted that the status then changes to Released. This forms the initial e-pedigree of the product item and nobody has the right to change or delete it. Tagged items are packaged and distributed based on order requirements from downstream supply chain nodes. The related order information and containment relationship information is similarly updated to the anti-counterfeiting system.

Supply chain nodes, such as wholesalers, distributors and retailers, mainly shoulder the responsibility to synchronize transaction information, as in the third step. When products are delivered to a warehouse center of a logistics company, the operator is firstly required to identify all the incoming garments utilizing proper RFID equipment (RFID-aided gate door, tunnel, handheld readers, etc.) and then authenticate the product items. The identification process can be facilitated by the containment relationship data and advanced order information. The detailed authentication mechanism is elaborated in next paragraph. Corresponding new Transaction Records would be composed and updated for successfully verified products, while any suspicious items would be screened out and Mark Fake data is synchronized. Product Containment Relationship may be changed and the items repackaged for further distribution, according to the specific need of product orders from downstream supply chain nodes. In retail shops, the cashier would generate the final Sale Record when a product item is sold by marking the record as Sold upon transaction confirmation, after which no further modification to the Sale Record is allowed. Product Release Updating and Transaction Recording are processed by the Authentication Server and the Pedigree Server cooperatively.

As mentioned in the previous paragraph, the automatic authentication mechanism executes the core concept of traceability anti-counterfeiting. Fig 4 shows the detailed logics and procedures. Authentication of a product item consists of four steps. The first three steps are aimed at checking whether the item has been ever Released by a manufacturer, or whether it has been marked as Fake, or whether it has been Sold before. The last step is to form the partial or whole geographical picture based on the item e-pedigree. If the result of any step is suspicious or implausible, the product item would be treated as illicit and then screened out. Both authentication request and transaction records synchronization are carried through SOAP requests.

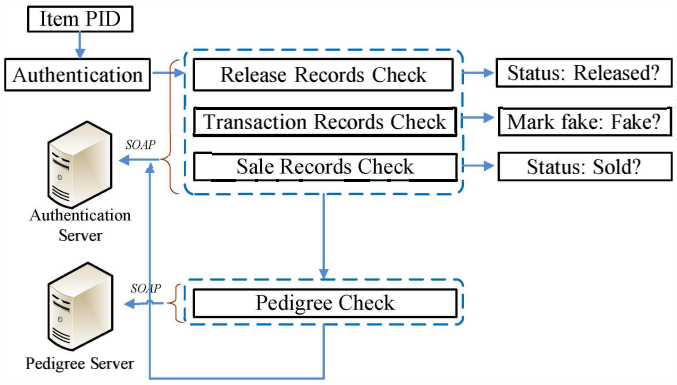

Figure 4. Automatic Authentication Mechanism

Overall, this synchronization mechanism and the authentication steps are all conducted by the system automatically without any human intervention, thus guaranteeing the credibility of the e-pedigree data and the reliability of the whole anti-counterfeiting system.

V. RBAC-BASED DATA VISIBILITY CONTROL MECHANISM

Synchronized and accumulated product e-pedigree data in the back-end databases may have to be checked or inspected (from time to time) by internal supply chain practitioners or government auditors for the purpose of after sale service or legal audit. In these scenarios, human interactions with the anti-counterfeiting system become inevitable; such interactions should be well-controlled to avoid possible data leakage/falsification or corrupting the entire system. Hence, a proper data visibility mechanism is needed to serve as an auxiliary module for the anti-counterfeiting system. In this section, we introduce a Role-based Access Control (RBAC) method and tailor it for our system.

As a quick review, RBAC was formalized in 1992 by F. David and Rick Kuhn in [20]. Now the family of RBAC is commonly referred to as the RBAC96 model [21]. The basic concept of RBAC can be described in Fig 5. Permissions including a variety of data operations (like adding, removing, and viewing) are assigned to roles based on specific policy rules rather than directly to individual users; users are assigned

to roles rather than directly to permissions. This level of indirection facilitates user-permission management to facilitate system access control.

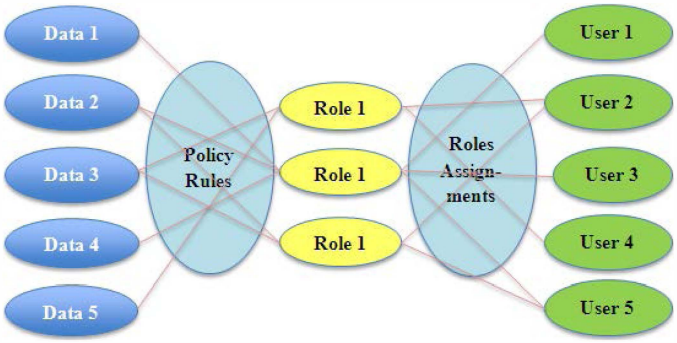

Figure 5. RBAC Diagram

To adapt RBAC for control of human interactions with the anti-counterfeiting system, different roles have to be defined. Each role is assigned a scope of data access/operation tasks. When supply chain employees, government auditors or licit third party outsiders attempt to interact with the back-end databases, those users are dynamically assigned one or more roles. The roles or privileges would be revoked immediately afterwards. Besides, all of these human interactions would be automatically logged in an individual table by the system. It should be noted that the total number of system roles and the scope of each role are defined based on the practical needs with reference to the apparel supply chain rules and the related business laws.

Overall, by limiting the privilege of accessing back-end databases, this RBAC-based access control module helps safeguard the security of back-end e-pedigree data, thus preventing possible data leakage/falsification.

VI. CONCLUSION AND FUTURE WORK

Based on an advanced RFID-aided track-and-trace anti-counterfeiting system architecture, we developed a comprehensive data structure for modeling apparel product e-pedigree, together with a mechanism for data updating and synchronization to guarantee the integrity and reliability of product e-pedigree data. One significant benefit of this data model is the enhancement of track-and-trace capabilities of product movement. By tracking information like item-level transaction records, pallet-level containment relationship, and batch-level order information, the system is able to verify individual item, detect missing/injected objects and predict products' future status at any location of the apparel supply chain. Further, we adapted RBAC mechanism visibility control of e-pedigree data to prevent possible data falsification and data leakage.

Overall, this paper has addressed the data management issues in RFID-based track-and-trace anti-counterfeiting. As future work, the proposed e-pedigree data model and the data synchronization/visibility mechanism would be implemented and evaluated in practical deployment settings.

REFERENCES

[1] Counterfeiting Coalition (IACC) http://www.iacc.org/. (Access date: 13 Novenber 2013) .

[2] Report of World Health Organization (WHO): Anti-counterfeit Technologies for the Protection of Medicines, http://www.who.int/impact/events/IMPACT-ACTechnologiesv3LIS.pdf. (Access date: 13 Novenber 2013).

[3] Ling Li, "Technology Designed to Combat Fakes in The Global Supply Chain", Business Horizons, Volume 56, Issue 2, 2013, pp.167-177.

[4] Mikko Lehtonen, "Description of The Status Quo of Existing Technical Countermeasures: their benefits and shortcomings", Version 1.01, 2009.

[5] Dipika Bansal, Swathi Malla, Kapil Gudala, Pramil Tiwari, "Anti-counterfeit Technologies: A Pharmaceutical Industry Perspective", Scientia Pharmaceutica, Volume 81, Issue 1, 2012, pp.1-13.

[6] EPCglobal Networks http://www.gs1.org/epcglobal. (Access date: 13 Novenber 2013).

[7] Alvin Cheung, Karin Kailing, Stefan Schonauer, Theseos, "A Query Engine for Traceability across Sovereign, Distributed RFID Databases", Proceedings of the 23rd International Conference on Data Engineering, Istanbul, Turkey, 2007.

[8] DIALOG: Distributed Information Architectures for collaborative logistics. http://dialog.hut.fi/. (Access date: 13 Novenber 2013).

[9] K. Främling and J. Nyman, "From tracking with RFID to intelligent products", In: Proceedings of 14th IEEE International Conference on Emerging Technologies and Factory Automation, Palma de Mallorca, Spain, 2009.

[10] R. Koh, E.W. Schuster, I. Chackrabarti, A. Bellman, "White Paper: Securing the Pharmaceutical Supply Chain", Auto-ID Labs, Massachusetts Institute of Technology, 2003.

[11] T. Staake, F. Thiesse, E. Fleisch, "Extending the EPC Network-The Potential of RFID in Anti-counterfeiting", ACM Symposium on Applied Computing, 2005, pp.1607–1612.

[12] T. Staake, F. Michahelles, E. Fleisch, J.R. Williams, H. Min, P.H. Cole, S.G.Lee, D. McFarlane, J. Murai, "Anti-counterfeiting and Supply Chain Security, Networked RFID Systems and Lightweight Cryptography", 2008, pp.33-43.

[13] J. Kim and H. Kim, "Anti-counterfeiting Solution Employing Mobile RFID Environment", World Academy of Science, Engineering and Technology, 2005.

[14] Mikko Lehtonen, Thorsten Staake, Florian Michahelles: "From Identification to Authentication-A Review of RFID Product Authentication Techniques", Networked RFID Systems and Lightweight Cryptography, 2008, pp.169-187.

[15] S.H. Choi, C.H. Poon, An RFID-based anti-counterfeiting system, International Journal of Computer Science, Volume 35, Issue 1, 2008, pp.1-12.

[16] BRIDGE http://www.bridge-project.eu/index.php/mainpage/en/, 2009. (Access date: 13 Novenber 2013).

[17] Jansen-Vullers, M.H., van Dorp, C.A. and Beulens, A.J.M, "Managing traceability information in manufacturer", International Journal of Information Management, Vol. 23, 2003, pp. 529-553.

[18] Ranasinghe, D.C., Cole, P.H., "Networked RFID Systems and Lightweight Cryptography: Raising Barriers to Product Counterfeiting". Springer, Berlin, 2008.

[19] Can-Trace Development for traceability standards for food products, http://www.can-trace.org/. (Access date: 13 Novenber 2013).

[20] David F. Ferraiolo and D. Richard Kuhn, "Role-Based Access Controls", 15th National Computer Security Conference, 1992, pp554-563.

[21] Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein, Charles E. Youman, "Role-Based Access Control Models", IEEE Computer, Volume 29, No.2, 1996, pp38-47.