International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:1, No:8, 2007

# Anti-Counterfeiting Solution Employing Mobile RFID Environment

Juhan Kim, and Howon Kim

***Abstract*—**EPC Class-1 Generation-2 UHF tags, one of Radio frequency identification or RFID tag types, is expected that most companies are planning to use it in the supply chain in the short term and in consumer packaging in the long term due to its inexpensive cost. Because of the very cost, however, its resources are extremely scarce and it is hard to have any valuable security algorithms in it. It causes security vulnerabilities, in particular cloning the tags for counterfeits. In this paper, we propose a product authentication solution for anti-counterfeiting at application level in the supply chain and mobile RFID environment. It aims to become aware of distribution of spurious products with fake RFID tags and to provide a product authentication service to general consumers with mobile RFID devices like mobile phone or PDA which has a mobile RFID reader. We will discuss anti-counterfeiting mechanisms which are required to our proposed solution and address requirements that the mechanisms should have.

***Keywords*—**EPC, RFID, Anti-Counterfeiting, Mobile RFID environment.

## I. Introduction

EPC™ Class-1 Generation-2 UHF (860-960 MHz) standard has recently ratified by EPCglobal which is the nonprofit organization charged with promoting the adoption of Electronic Product Code (EPC) technology. This defines the physical and logical requirements for a passive-backscatter, Interrogator-talks-first (ITF), radio-frequency identification (RFID) system operating in the 860 MHz – 960 MHz frequency range. The system comprises Interrogators, also known as Readers, and Tags, also known as Labels. An Interrogator interacts with a Tag by modulating an RF signal in the 860 MHz – 960 MHz frequency range. The Tag receives both information and operating energy from this RF signal. Tags are passive, meaning that they receive all of their operating energy from the Interrogator's RF waveform [1, 2].

Thanks to relatively inexpensive cost to the tags, ideal estimate is 5 cents in next several years [15], it is expected that most companies are planning to use it in the supply chain in the short term and in consumer packaging in the long term.

Because of the very cost, however, its resources are extremely scarce and it is hard to have any valuable security algorithms in it. It causes security vulnerability, in particular cloning the tags for counterfeits.

Counterfeiting is one of the fastest growing economic crimes worldwide. It threatens the economies of developed and developing countries alike, undermines trading relations, scares off vital new investment, and increasingly endangers public health and safety. Counterfeiting has spread at an alarming rate to electrical and electronic goods and components, machines and equipment, spare parts of all types, pharmaceuticals [10] and even high technology products. Counterfeit products account for between 5-7% of world trade [20].

In this paper, we propose an application level solution against counterfeiting. It aims to become aware of distribution of spurious products with fake RFID tags and provide product an authentication service to general consumers with mobile RFID devices [18] like mobile phone or PDA which can connect mobile RFID readers [4, 16] which are made especially for the mobile phone and the PDA. Targeted RFID tags are compliant with EPC Class-1 Generation-2 UHF standard that is expected that most companies are planning to use it in the supply chain.

Our concern is not security techniques of tag-reader level to prevent cloning tags but tag-application level methods to provide a mobile service for users to check products' originality and for manufacturers to detect counterfeits by the mobile service. With the service and supply chain management system they have, manufacturers can find out where the counterfeits are and which distribution channels are in problem. As a result of the processes, it is possible to prevent mass distribution of the counterfeits.

In our solution, we employ contexts from mobile environment and watermarking technologies for authenticating consumer products. When a consumer requests a product authentication to a product authentication application with her mobile RFID device, she must send an EPC from a tag and a watermark-embedded image on the product capturing by her digital camera in the device. The product authentication application gathers information such as the EPC, the watermark extracted from the image, location information from LBS (location-based Service) providers, and owner-ship information from SCM or her device. Then, it compares them with those from the application database managing EPCs, watermarks and contexts history per EPC. Ac-cording to the comparison, the application returns its authentication result to the consumer's device by sending a product certificate that comprises of the authentication result like 'a real article', 'not real article', or 'can not authenticate', date of issue, date of

Juhan Kim and Howon Kim are with the Electronics and Telecommunications Research Institute (ETRI), 161 Gajeong-dong, Yuseong-gu, Daejeon, 305-350, Korea (e-mail: juhankim, howonkim@ etri.re.kr).

expiry, information about the product and digital signature of the application.

As we have described above, we suggest that anti-counterfeiting solution that has a mobile service for authenticating a product by EPC, watermark and contexts from the supply chain to the mobile RFID environment. With EPC, the product authentication application accumulates contexts history in each distribution step of supply chain. With the watermark, it can provide restrict access and auxiliary authentication method for consumers to authenticate the very products that the consumers want to know irrespective of places.

We present an overview of the EPC, EPCglobal network, mobile RFID environment and related works in section 2. In section 3, we propose anti-counterfeiting solution and we conclude in section 4.

## II. Background

The EPC was created by the Auto-ID Center as an eventual successor to the bar code. The aim was to create a low-cost method of tracking goods using RFID technology. The benefit of RFID is that it doesn't require line-of-site, which means goods can be scanned through packaging and without needing people to scan items. EPC tags were designed to identify each item manufactured, as opposed to just the manufacturer and class of products, as bar codes do today [12].

### A. EPC Network

EPCglobal is a joint venture between EAN International and the Uniform Code Council (UCC). It is a not-for-profit organization entrusted by industry to establish and support the EPC Network as the global standard for immediate, automatic, and accurate identification of any item in the supply chain of any company, in any industry, anywhere in the world. Its objective is to drive global adoption of the EPCglobal Net-work [12].

The EPCglobal EPCglobal Network consists of five fundamental elements [17]:

1) EPC: The EPC is a globally unique serial number that identifies an item in the supply chain. This allows enquiries to be made about a single instance of an item, wherever it is within the supply chain.
2) The ID System: The ID System consists of EPC tags and EPC readers. EPC tags are RFID devices that consist of a microchip and an antenna attached to a substrate. The EPC is stored on this tag, which is applied to cases, pallets and/or items. EPC tags communicate their EPCs to EPC readers using Radio Frequency Identification. EPC readers communicate with EPC tags via radio waves and deliver information to local business information systems using EPC Middleware.
3) EPC Middleware: EPC Middleware manages real-time read events and information, provides alerts, and manages the basic read information for communication to EPC Information Services as well as a company's other existing information systems. EPCglobal is developing a software interface standard for services enabling data exchange between an EPC reader or network of readers and information systems.
4) EPCIS: EPC Information Services enables users to exchange EPC-related data with trading partners through the EPCglobal Network.
5) Discovery Services: The Discovery Services is a suite of services that enables users to find data related to a specific EPC and to request access to that data. The Object Naming Service (ONS) is one component of the Discovery Services.

### B. Mobile RFID Environment

In this paper, mobile RFID environment means that mobile RFID devices [4, 16] like mobile (cellular) phone and PDA employing cellular network can be used at querying information of the consumer product related a tag [19]. The mobile RFID devices should have mobile RFID readers which are made for them and are, in particular, compliant with EPCTM Class-1 Generation-2 UHF (860-960 MHz) standard [18]. That is, Class-1 Generation-2 tags mainly for supply chain are also used for consumer products. Thus, any consumer can get information of a product with a tag by sending an EPC of the tag to an EPC information server with her mobile RFID device in this mobile RFID environment.

### C. Related Works

Legacy approaches like Juel [5, 6, 8, 9], Molnar [7] and Golle [11] are focused on making techniques which are impossible to clone tags by proving secure channel between tags and readers, or between tags and database. Those approaches, however, are hard to be employed at EPCTM Class-1 Generation-2 UHF (860-960 MHz) compliant tags because of limited resources the tags except Juel [8].

Quiet briefly, Juel [8] makes use of kill PIN and access PIN for authentication by sending those PINs to a tag and analyzing responses from the tag. The kill PIN is a password for consumers' privacy by killing the tags operation completely and permanently and the access PIN is used to access data bank in the tag.

The Juel's approach is very useful in supply chain. However, it is not suited for authenticating products by consumers' mobile RFID devices, because the PINSet for PIN-test for authentication are easily exposed to the consumer's mobile RFID device. Once any adversary with a mobile RFID device requests information of the product with a tag to a centralized server, she can get the PINSet with her mobile RFID device during the interaction of the tag and the server. Then she can kill the tag easily by sending PIN one by one in the PINSet. It is because the number of PINs in the PINSet is quite smaller than combination number of the kill-PIN consists of 32 bits.

Staake [3] proposed EPC-PAS (Product Authentication Service) for anti-counterfeiting which can track and trace the movement of goods from production to consumption and which employs secure authentication in a Database-Reader-Tag environment like Fig. 1. The secure

authentication, however, cannot be applied the tags compliant with the standard.

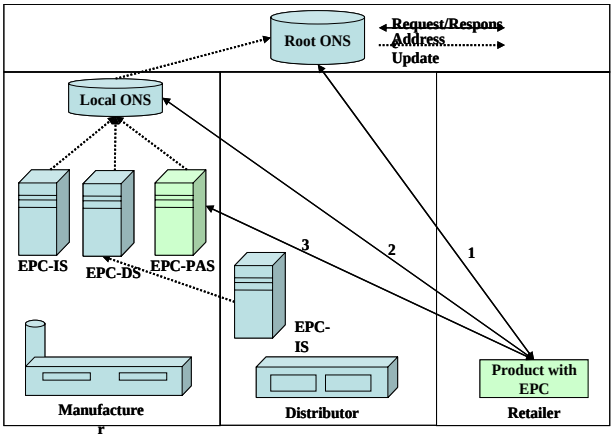


Fig. 1 Staake's evolving EPCglobal network including the EPC-PAS for anti-counterfeiting

## III. Proposed Anti-Counterfeiting Solution

The reason that we employ Class-1 Generation-2 standard is because it is expected that most companies are planning to use it in the supply chain and in packaging consumer products at the same time. Mobile RFID readers for consumers, which are used to read such consumer products that are compliant with the standard, are now developing and recently a mobile RFID reader for PDA like IP4 [18] is launched. In this paper, we assume that a mobile RFID device is kind of mobile phone or PDA that can be connected to CDMA or GSM network and has such a RFID reader.

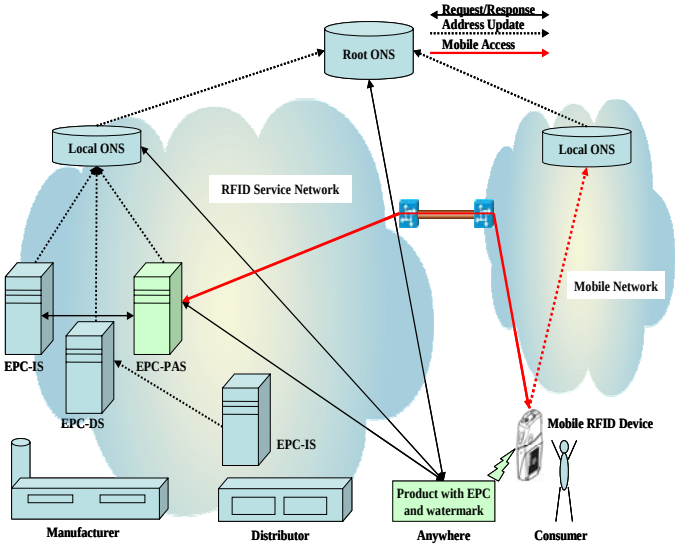


Fig. 2 The EPC infrastructure we are evolving for anti-counterfeiting which is irrespective of the location of a product with a tag

### A. Mobile RFID Environment

Thanks to above devices, it is possible to track and trace a product during whole life-cycle of typical RFID tag that consists of four main phases such as supply chain, point-of-sales, customer control & after sales service, and recycling & waste management. In the mobile RFID environment that the mobile RFID devices can be used at, the EPC-PAS can track and trace a product with a tag whenever a consumer requests information of the product with her mobile device.

In this respect, it is expected that manufactures can get a powerful means to prevent mass distribution of counterfeits with only extending ability about tracking and tracing to the mobile RFID environment like Fig. 2. Therefore, even if there are counterfeits at markets which is not covered with the supply chain, manufacturers can find out them and which distribution channels are in problem as soon as any consumer requests information of the product with a tag. As a consequence, it is possible to prevent mass distribution of the counterfeits and improve the distribution channel for anti-counterfeiting. However, from the viewpoint of consumers, there is new vulnerability like the following scenario in the mobile RFID environment;

- If there are many consumer products having EPC tags. Only several tags are real and most of them are fakes (fakes are only imitation of the real tag's appearance). A consumer will identify a product with her mobile RFID device and she can get a message it is a real thing. However, she may not know exactly where the real thing is because anticipated recognition distance of her mobile RFID device, which compliant with Class-1 Generation-2 standard, reaches 0.5M ~ 3M. In particular, if she asks to kill the tag related the product for her privacy; the problem will be more serious because the retailer can sell an unproved product to her without any effort.

Above scenario is caused by that mobile RFID readers have a few restrictions com-pared with legacy wired RFID readers. The readers can recognize merely several tags at once, and it will cost to identify each EPC of the tags through CDMA or GSM network. Therefore, we do not believe that a consumer would be willing to identify all products in front of them and that she could always choose an authenticated product among many products in above scenario.

### B. The EPC-PAS

In proposed works, the EPC-IS supports an interface for mobile RFID devices. The EPC-IS that receives a request from the consumer invokes the EPC-PAS for product authentication in Fig. 3.

Then the EPC-IS gets the result from it and sends information of the product with the result to the consumer and it accumulates the location to build historical locations for tracing a product. The EPC-PAS has an LBS client for taking location information from LBS providers and provides alert service to warn manufacturers of discovering the counterfeits.

The EPC-PAS gathers only contexts while a product with a tag is in supply chain without any consideration about

watermark embedded in an image on the product.

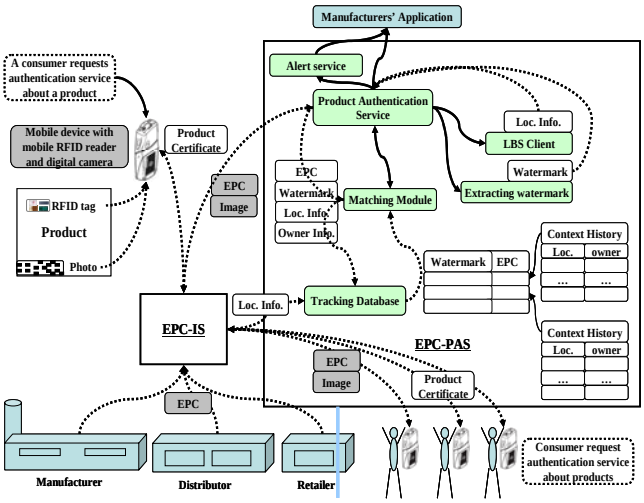


Fig. 3 The dataflow in the EPC-PAS which has a product authentication service for consumers and an alert service for manufacturers

However, it utilized the watermark to authenticate the product that are in the mobile RFID environment, it also accumulates contexts like location from LBS providers and ownership from consumers' devices or supply chain management systems whenever the consumers query about information of the product. Then it returns a certificate which comprise of the authentication result like 'a real article', 'not real article', or 'can not authenticate', date of issue, date of expiry, destination information, product information and PKI-based digital signature [21] of it. Mobile RFID devices for consumers, therefore, should support functions that can identify manufacturer and check integrity of the certificate by verifying the signature. It should also check validation date in the certificate.

Therefore we will address separated two kinds of authentication mechanisms for each environment. One, Juel's approach [8] like Fig. 4, is for the supply chain that is, in this paper, interacted with only trusted readers.

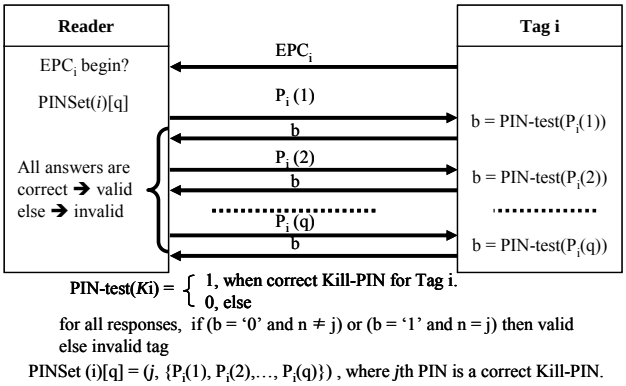


Fig. 4 Authentication protocol between a reader and a tag for anti-cloning

The other, digital watermarking technology is for the mobile RFID environment that untrusted mobile RFID devices will be connected to.

Juel's mechanism, as we have explained in related works, utilizes kill PIN in authentication by sending the PINs to a tag and analyzing responses from the tag that has additional function, PIN-test. It is very useful in the supply chain that interacts with only trusted readers because it is possible to authenticate a tag with quiet small PINset.

However, it is not suited for authenticating products by consumers' mobile RFID devices, because the PIN-test set from authentication are easily exposed to the consumers' mobile RFID devices. An adversary can kill the tag easily by sending PINs one by one in the PINSet. It is because the PINSet could not have enough PINs due to time and cost at mobile network.

Digital watermarking technology, which is hiding information for proving owner-ship for digital contents in cyberspace, is useful to restrict access to avoid the above vulnerability as stated in 3.1. In particular, for consumers in mobile RFID environment that is not fixed areas like the supply chain and can be anyplace consumers are, an ability of accessing to a targeted product accurately is more important than automatic identification about incorrect products including the target because of the cost to use mobile network. In this respect, the watermarking can be an alternative as an auxiliary authentication medium in the mobile RFID environment. This kind of watermark approach is similar with it for secure ID card solutions for personal identification [23].

Digital watermarking scheme for anti-counterfeiting that should have properties like this: it should have a covert and different watermark in every image, it should be robust to rotation and scaling of image from consumer's device, and it could differentiate sharply between watermarks of original labels from watermarks of fake images that are made by capturing the original label and reprinting the original. The ability for differentiation is very important in this paper because the watermarking is used to authenticate a product in the mobile RFID environment.

Quality of fake image made by scanning and reprinting is generally worse than it of original, and the watermark from fake image will be much different with it of original. Therefore, the threshold to make a decision that an image is original should be enough high for the EPC-PAS to distinguish exactly the fake image from the original.

To distribute counterfeits with fake tags and image massively, an adversary needs to capture images and make fake tags on many products. If she could make counterfeits with fake tags and images, she could not distribute them. It is because the counterfeits will be discovered as soon as a consumer requests information of one of the counterfeits due to the counterfeit's location that is different with it of the original in the EPC-PAS. And from an LBS provider, a manufacturer can get exact location information where the consumer is and prevent their

distribution. The manufacturer can also trace distribution channel by analyzing accumulated history contexts in the EPC-PAS.

### C. Other Security Considerations

The EPC-PAS in the proposed model issues a certificate which is including authentication result, date of issue, date of expiry, destination information, information of the product and PKI-based digital signature for all of them. Therefore, consumers' devices should support security mechanism such as cryptography algorithms for digital signature of PKI. They also message level security mechanisms like message encryption algorithm for transmit messages securely to the EPC-PAS.

## IV. Conclusion

We proposed an application level anti-counterfeiting solution that can track and trace a product through whole lifecycle of EPC tag with upcoming consumers' mobile RFID devices like mobile phone or PDA with a mobile RFID reader. We also suggested the extension of the EPC-PAS to cover mobile RFID environment for tracking and tracing a product continuously with an EPC tag irrelative of places whenever a consumer requests information of the product with her mobile RFID device. Therefore, even if there are counterfeits at market, manufacturers can find out them and which distribution channels are in problem as soon as any consumer requests information of a counterfeit with a fake tag.

We also discussed anti-counterfeiting mechanisms such as Juel's anti-cloning approach for the EPC tag and digital watermarking technology which are required to our proposed solution and addressed requirements that those mechanisms should have.

Future research will address the watermarking scheme in detail, the structure and security of mobile RFID device, and security mechanism that can be applied to both the supply chain and the mobile RFID environment.

## References

[1] EPCglobal Web site. www.epcglobalinc.org, 2005.
[2] EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz Version 1.0.9 ttp://www.epcglobalinc.org/stan-dards_technology/EPCglobalClass-1Generation-2UHFRF-IDProtocolV109.pdf
[3] Thorsten Staake, Frédéric Thiesse, Elgar Fleisch. Extending the EPC Network – The Potential of RFID in Anti-Counterfeiting, In Proceedings of the 2005 ACM symposium on Applied computing, pages 1607 – 1612, ACM, 2005.
[4] Nokia unveils RFID phone reader. RFID Journal, 17 March 2004. Available at http://www.r-fidjournal.com/article/view/834/1/13.
[5] Ari Juels. Minimalist cryptography for low-cost RFID tags. In C. Blundo and S. Cimato, editors, Security in Communication Networks (SCN 04), pages 149–164. Springer-Verlag, 2004. LNCS no. 3352.
[6] Ari Juels. 'Yoking-proofs' for RFID tags. In PerCom Workshops 2004, pages 138–143. IEEE Computer Society, 2004.
[7] David Molnar and David Wagner. Privacy and Security in Library RFID : Issues, Practices, and Architectures. In B. Pfitzmann and P. McDaniel, editors, Computer and Communica-tions Security, pages 210 – 219. ACM, 2004.
[8] Ari Juels. Strengthening EPC Tags Against Cloning. Available at http://www.rsasecu-rity.com/rsalabs/staff/bios/ajuels/publications/pdfs/EPC_authentication-16Mar05.pdf
[9] Ari Juels and Ravikanth Pappu. Squealing euros: Privacy protection in RFID enabled bank-notes. In Rebecca N. Wright, editor, Financial Cryptography – FC'03, volume 2742 of Lecture Notes in Computer Science, pages 103–121, Le Gosier, Guadeloupe, French West In-dies, January 2003. IFCA, Springer-Verlag.
[10] U. S. Department of Health and Human Services, Food and Drug Administration (2004) Combating Counterfeit Drugs, A Report of the Food and Drug Administration. Available at http://www.fda.gov/oc/initiatives/counterfeit/report02_04.pdf.
[11] P. Golle, M. Jakobsson, A. Juels, and P. Syverson. Universal re-encryption for mixnets. In T.Okamoto, editor, CT-RSA '04. Springer-Verlag, 2004.
[12] RFID Journal Frequently Asked Questions, http://www.rfidjournal.com/faq.
[13] Mobile RFID Forum, http://www.mrf.or.kr.
[14] Stephen A. Weis, Sanjay E. Sarma, Ronald L. Rivest, and Daniel W. Engels. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In Security in Pervasive Computing, volume 2802 of Lecture Notes in Computer Science, pages 201-212, 2004.
[15] The 5-Cent Challenge. RFID Journal, 30 August 2004. Available at http://www.rfidjou-rnal.com/article/articleview/1100/1/2/.
[16] Test Set for RFID-Enabled Phones. RFID Journal, 20 September 2004. Available at http:// www.rfidjourn-al.com/article/articleview/1125/1/20/.
[17] About the EPCglobal Network™. Available at http://www.epcglobalinc.com/about/about _epc_network.html.
[18] IP4 Portable RFID Reader. Available at http://www.intermec.com/eprise/main/Intermec/C-ontent/Products/Products_ShowDetail?Product=RFID2_IP4
[19] Mobile RFID Forum' Launched. IT Korea Journal March~April 2005, page 61. Available at http://www.ica.or.kr/lib/ITKorea_Eng(0503)/052%20industry%20news.pdf
[20] The International Anti-Counterfeiting Directory 2003. ICC Counterfeiting Intelligence Bureau. Available at http://www.iccwbo.org/ccs/cib_bureau/CIBDirectory.pdf
[21] RSA Laboratories. What is the RSA cryptosystem? Available at http://www.rsasecurity.co-m/ rsalabs/node.asp?id=2214.
[22] Mauro Barni and France Bartolini. Data Hiding for Fighting Piracy. In IEEE Signal Processing Magazine, March 2004, page 28 ~ 39.
[23] Digimarc. Enhancing Personal Identity Verification with Digital Watermarking, Available at http://csrc.nist.gov/piv-program/FIPS201-Public-Comments/digimarc.pdf
[24] Stephan J. Engberg, Morten B. Harning, Christian Damsgaard Jensen. Zero-knowledge Device Authentication: Privacy & Security Enhanced RFID preservingBusiness Value and Consumer Convenience, In Proceeding of PST 2004, page 89~100.