Hadi M. Saleh, Mohammed U. Umaru, Dmitry V. Alexandrow

Protection System Against Products Counterfeit Based on NFC and Barcode Technologies

Edukacja - Technika - Informatyka nr 4(22), 368-374

2017

© Wydawnictwo UR 2017 „Edukacja – Technika – Informatyka” nr 4/22/2017
ISSN 2080-9069 www.eti.rzeszow.pl
ISSN 2450-9221 online DOI: 10.15584/eti.2017.4.50

HADI M. SALEH[1], **MOHAMMED U. UMARU**[2], **DMITRY V. ALEXANDROV**[3]

Protection System Against Products Counterfeit Based on NFC and Barcode Technologies

[1] Ph.D., associate Professor, Vladimir State University n.a. A.G. and N.G. Stoletovs, Russia
[2] Master Student, National Research University Higher School of Economics, Russia
[3] D.Sc., professor, National Research University Higher School of Economics, Russia

Abstract

The objective of this report is to provide a protective system architecture and analysis for NFC and Barcode technology that can be use to empower consumer in the fight against counterfeiting and IPR infringing products using mobile devices. This report focuses on the technology that can empower the consumer in the field in the presence of the goods itself by using technical tools and devices, which are easily available. The report identifies the main immediate empowerring tool for consumers. This is represented by a modern smartphone (or similar device like a tablet) to be use as a tool to empower the consumer in the fight against counterfeiting. The modern smartphone is equipped with a high resolution camera, support for different standards for wireless connectivity, a powerful processor able to support the implementation of sophisticated algorithms and support for NFC and Barcode readers. In addition, the smartphone can be integrated and augmented with a wide range of plug-in devices and tools (e.g., an USB microscope). The concept of empowering the consumer can be an important element to support Due Diligence practices and Supply Chain Integrity because the different categories of consumer can authenticate the goods in different parts of the supply chain and report the presence of non-compliances (e.g., counterfeit products).

Keywords: Anti-Counterfeit Products; NFC Tags; Barcodes; QR, Mobile Application; Authentication; Near Field Communication (NFC)

Introduction

Products counterfeiting isn't a brand new drawback, however, the circulate distribution of faux product is still a worldwide drawback and also the scope of merchandise subject to encroachment has enlarged altogether. For instance, clothing industries has witness a higher percentage of more than 50% of the faux product confiscated by U.S Customs and Border management. As indicated by the investigation of Counterfeiting Intelligence Bureau (CIB) of the International Chamber of Commerce (ICC), faux product made up to five to seven- percent of

World Trade, but these figures cannot be corroborated as a result of the hidden manner of the trade (ICC, 1997). The foremost basic methodology, printing a faux label with a subtly misspelled name or a rather completely different emblem in hopes of casual product customers, has been common to different luxury--goods markets liable to counterfeiting. A lot of formidable counterfeiters would possibly take away associate authentic label and place it on a bottle or product packages with the same form. NFC and Barcode technology have been analysed, investigate and introduce as a single tool technology for anti-counterfeiting (NDEF, 2016). But yet still, they come have certain pitfalls that make it difficult for the consumers to use which then enable the counterfeiters to continue their illicit trade. The projected system is geared toward comparatively high-end client product and it helps defend real product by maintaining the merchandise pedigree like the dealings records and also the offer chain integrity due to its multiple features. As such, purchasers can safeguard their stake by authenticating product with their enabled smartphones with either NFC or Barcode before making payment at retail points using the help of mobile application.

Counterfeit products are classified into four classes:

1) The primary class consists of these products that are cheap, lower quality and will lack original packaging.

2) Within the second class of counterfeit, reverse designed and identical products are copied and are sold-out because the genuine product is arduous for a client to differentiate between a real and a counterfeit product.

3) Within the third class, the products are created by associate outsourced manufacturer while not imitating the first owner. For instance, associate outsourced manufacturer manufactures more products when terminating its contract with the first owner while not notifying the first owner.

4) Lastly, these classes are real product that don't meet the manufacturer's standards however aren't labelled as faulty.

The circumstances of counterfeit product spreading involve a lot of mechanisms to fight counterfeiting by enhancing the prevailing system. The purpose of this work relies on empowering the client which is a crucial part to support Due Diligence practices and provide Chain Integrity as a result of completely different classes of consumer that will check for the product authenticity within the scope of the distribution chain and report the presence of non- counterfeit products. Category 4 counterfeits can be restricted by enforcing an efficient quality control measure by the genuine product owner. Categories 2 and 3 are most critical as not only is the consumer unaware of the illegitimacy of the product, but also the genuine owner has no or minimal control over the production, marketing and selling of such products. Our model helps in detecting counterfeits products at consumer level pertaining to category 2 and 3 products, thus providing an

efficient tool to detect counterfeits by using Barcode and NFC technology to improve current authentication methods processes of illicit trade.

Our solution model provides a design architecture of a client based that enables customers at different level of the supply chain to authenticate their purchased products in a more easy and convenient manner using mobile application on their enable smartphones. In our proposed solution structure, customers have two optional multi-function barcode and NFC reading technology designed to capture, parse and validate specifically targeted data embedded within a single barcode or tag. Thus, when the smartphone of the customer is not an NFC enable the customers can still authenticate the product with his/her phone that has the barcode feature. Also, the customer can authenticate NFC embedded product with his/her NFC enable device using the NFC option on his mobile application.

This technology builds upon the codeREAD platform's dual function QR code technology which allows a single QR code to be used for both consumer engagement and enterprise asset tracking. The platform's multi-function technology enables workflow-specific asset tracking and validation of a much larger number of IDs in a single QR code or NFC tag and also enables the use of DataMatrix, PDF417 and MaxiCode 2D barcode symbologies. Using the codeREAD, there are some assign specific tasks for app-users. For each task defines which IDs need to be parsed from the string of IDs embedded in the barcode or tag. The parsed IDs are checked against a table of valid IDs hosted on codeREAD's servers, a client's servers. If the target ID or combination of target IDs exists in the table, the app user will see a valid response and information specifically related it; if it's not in the table, the response will be invalid. In either case, the app-user can be prompted to collect additional information with each scan which, along with a timestamp and optional GPS location, all becoming part of a formal scans record. With this proposed technology enterprises can save money and space by combining multiple authentication tools such as 'valid' ID to be embedded in a barcode or NFC target into a single label. It also improves data collection accuracy because the app parses the correct information based on the specific task, not on which barcode or NFC tag is scanned.

In the context of the fight against counterfeiting, the smartphone itself is the component (in the hand of the consumer) of a wider system, which can include an application, a communication protocol, a reference library, a brand-owner database of the product features, or a database linked to the supply chain and other elements. The smartphone is used to collect data (NFC, or Barcode tag embedded) from the goods to be evaluated, this knowledge will be processed on the smartphone itself (e.g., to extract features) to get further info from the database associate application. The smartphone sends the data and also the information to cloud storage application for the verification of the product. When the product item is verified as true, the person/user gets a fulfilment message with

information of the specific product that includes date of manufacture and expiring date. However, while the product item is fake, the consumer gets a failure message through the app. The verification of the products will then be saved in the app's history and the consumer has the option of sharing the information of the detected counterfeit product on Social Media such as VK or Facebook.

Main elements of smartphone-based approach for the fight against counterfeiting of products are smartphone application, communication protocol, remote application and cloud service. Smartphone Application can even implement specific algorithms method and it may extract applied math options from the retrieved knowledge. It is furtherly accountable for causing the information (e.g., features, position or privacy settings) to the remote application employing a well-outlined communication protocol. Communication protocol is accountable for causing the info and knowledge from the smartphone application to the remote application and causing back the response from the remote application to the smartphone application. Remote application can be hosted on an overseas server that additionally uses the communication protocol to exchange knowledge with the smartphone application. The remote application uses the information from a reference library to judge if the received data from the smartphone is counterfeit or not. Cloud Service provides the system with the info required for matching (e.g., track and trace for product identifications), which may be created by the brand-owner itself or by associate external company that is ready to gather from the brand-owner the knowledge establish the valid product victimization NFC tag or barcode. This generic progress is diagrammatic within the following figure:

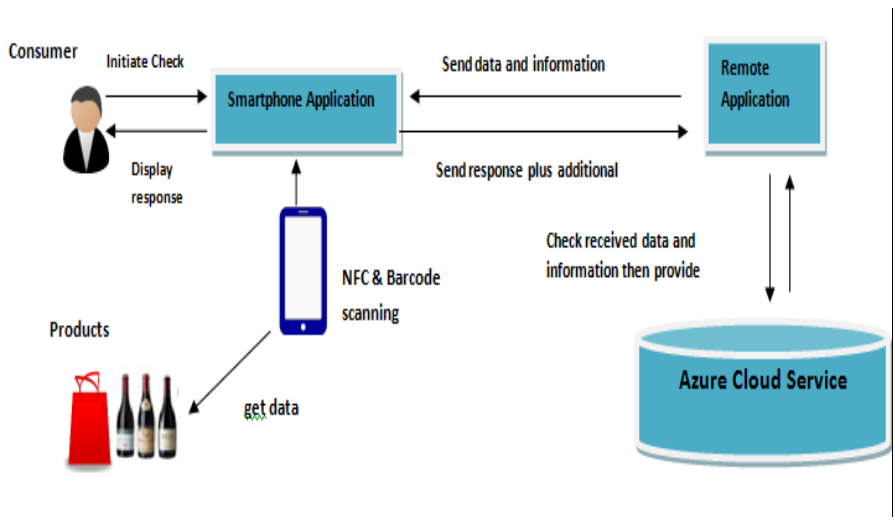

Figure 1. Generic progress

The **NFC Barcode** is a proposed design of a printed integrated circuit (PIC) for use in electronic read-only transponders. It is designed suppose to operate at 13.56MHz. The NFC Barcode operates in a Tag-Talks-First (TTF) mode, repeatedly transmitting its code at a specific interval as long as it is powered up. It adheres to a subset of the ISO 14443 Type A RFID standard. The NFC Barcode supports single-tag read mode (Ali *et al.*, 2005).

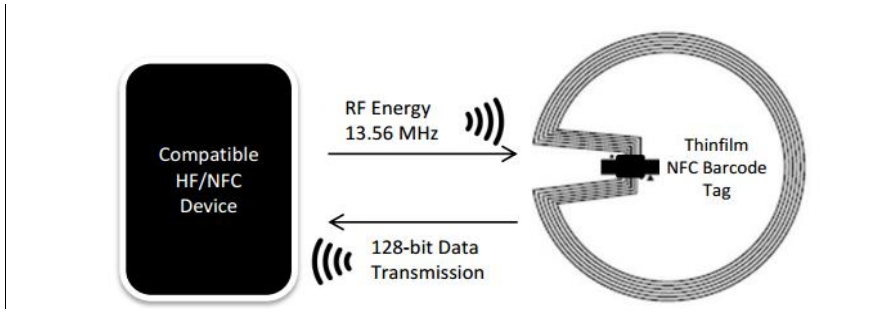

Figure 2. Operation overview

NFC devices communicate via magnetic field induction whereby the loop antenna of the reader device and the loop antenna of the NFC device are located within each other's near field, effectively forming an air-core transformer. By such a configuration, it is possible to transmit data and power from one device to the other (Bilcare, 2015).

Specifically, NFC Barcode is a type of NFC tag, which is an RF barcode-type device and comprises a printed integrated circuit (PIC) comprising an antenna, a master circuit, a transponder and a 128-bit ROM. The ROM is loaded with a unique identification code (UID), and the device operates in a passive, read-only mode. As such, when the RF barcode device enters the RF field of a reader device, it is powered-up and by an induction current in its antenna, and then proceeds to broadcast its 128-bit code (the UID) at intervals. In other words, the RF barcode device operates in a Tags-Talk-First (TTF) mode, it does not accept any commands from a reader but rather, as soon as it receives enough power from the reader's field to operate, it repeatedly transmits its UID at a specific interval, as long as it is powered (Resonant Coupling…). The sequence commences by switching ON the RF field, whereupon the ISO 14443-3 polling loop protocol is initialized. During the seek procedure, a guard time of 5 ms is waited-out. If an RF barcode device is present in the RF field, i.e. if the NFC reader receives the 1st bit before the expiry of the 5 ms guard time, then the RF barcode device is deemed “detected” and the remainder of the UID is obtained. On the other hand, if 5 ms guard time expires without detecting an RF barcode device, then the NFC reader will proceed to poll for NFC-A devices in the usual

way. NFC reader will proceed to poll for NFC-A tags only if it does not detect an RF barcode device within 5 ms of switching ON the RF field. A need therefore exists for a solution that makes it possible for RF barcode-type devices to coexist with other types of NFC devices in an NFC environment, for example, enabling RF barcode devices and other ISO 14443-compliant devices to cohabit and interoperate in parallel with a common reader device.

Conclusions and Future Discussion

To sum up, we tend to achieved all the objectives by the end of this project, represented in the paper the "Objectives of Implementation", during which the objectives like understanding the background of the rampant counterfeiting scenario in Russia and even within the world, planning the general structure and communication mechanism between completely different elements of the system and building solid models for elements just like the Azure info, the Scanning and also the Tag/Barcode with compatible smartphone. It is fair to comment that the project has been progressing with success because the solid model we'll be operating with might eventually be made, tested with completely different things, just like the scenario once the NFC tags/Barcodes were being cloned by counterfeiters, and even incontestable to the general public for more enhancements on the safety thought and also the aesthetic values on the final layout of the database and applications. The protection system design and analysis for NFC Barcode technology project is being analysis and a planned system shall be developed, specifically supported by customary software system development life cycle named as Development Life-cycle, during which the total development method was really commenced at a stage of drawback definition during which the international product counterfeiting scenario, the restricted effectiveness of existing labelling technologies were known and noted per those literature reviews, giving sturdy incentives to style associated build an anti-counterfeiting system, mistreatment NFC Barcode, below that the labelling technology has never been applied for this purpose. At the tip of this paper, the elements just like the applications and info are going to be style and develop once all the need definition and analysis of various elements were done. All the elements can then be connected along through planning APIs at the applying development tools and programming functions enclosed within the "AppController" of the web-based info. The prototyped shall then place to check so the foremost appropriate NFC tag/barcode operating with the system might so be determined and adopted for a series of demonstrations to supervisors and potential users.

Recommendations:1): A common standard to empower the consumer for good authentication through a smartphone should be developed. 2): Create an expert group for the analysis of new empowerment techniques appearing in the market. 3): Implement an awareness knowledge management repository at Eu-

ropean level in collaboration with retailers and manufacturers to be used and accessed through smartphones. 4): Implement a cost/benefit analysis to implement authentication technology to support empowerment of the consumer in specific domains. 5): In the definition of Due Diligence and Supply Chain Integrity processes to fight against counterfeiting, the role of empowerment of the consumer should be clearly defined.

References

Ali *et al.*, (2005). A New Circularly Polarized Rectenna for Wireless Power Transmission and Data Communication. *Ieee Antennas And Wireless Propagation Letters*, *4*.

Bilcare (2015). Smart Devices by Adrian Burden at Bilcare Technologies. Retrived from: http://www.bilcaretech.com/pdf/whitepaper/Technology-has-a-habit ofconverging.pdf (8.2015).

ICC (1997). *Countering Counterfeiting: A Guide to Protecting and Enforcing Intellectual Property Rights*.

NDEF (2016). Retrived from: ibadrinath.blogspot.com/2012/07/nfc-data-exchange-format-ndef.html (13.09.2017).

PC World. *NEC Smartphone Tech Can Spot Counterfeit Goods*. Retrived from: http://www.pcworld.idg.com.au/article/559250/nec-smartphone-tech-can spotcounterfeit-goods/ (10.11.2014).

Resonant Coupling. Retrived from: web.archive.org/web/20120930022841/http://www.wirelesspowerconsortium.com/technology/resonant-coupling.html (13.09.2017).