International Journal of Advances in Computer Networks and Its Security– IJCNS
Volume 5: Issue 2 [ISSN : 2250-3757]
Publication Date : 30 October, 2015

A Study on the Efficient NFC-based A Forgery Prevention Method

Eun Kim, Su Jin Lee, Hyun Joo Yoo, Jung Won Choi, Seong Jeen Kim, Min Soo Jung

***Abstract*—Today, scale of counterfeit goods market is growing continuously. Thus, the way to verify the legitimate product is required. Earlier authentication methods are difficult for the verification from the user side. In this paper, we propose an efficient method for the forgery prevention.**

***Keywords*—Forgery Prevention, Authentication, NFC**

I. Introduction

Nowadays, damage accidents that there are distributed to forge with a famous genuine things by malicious operator are increasing constantly. And also, side of product manufacturer, they produce authenticated product by applying like a barcode, RFID, Hologram and etc. However, users are difficult to recognize the legitimate product such that the only way. For this reason, users want to know the correct information about the product they are buying. Therefore, we believe that can perform to authenticate safely by using stored authentication information in the server of AuC. And the more convenience method may be used by using a smart phone and NFC technologies. Thus, we propose an efficient NFC-based a forgery prevention method. And this time, a NFC-equipped smart phone and the authentication application are authentication tools. And we design to store authentication information in physically strong USIM file system.

Eun Kim/Kyungnam University
Kyungnam University
Changwon-si

Su Jin Lee/Kyungnam University
Kyungnam University
Changwon-si

Hyun Joo Yoo/Kyunganm University
Kyunganm University
Chanwon-Si

Jung Won Choi/Kyungnam University
Kyungnam University
Changwon-si

Seong Jeen Kim/Kyungnam Univeristy
Kyungnam University
Changwon-si

Min Soo Jung/Kyungnam University
Kyungnam University
Changwon-si

II. Related Work

A. *NFC(Near Field Communication)*

The NFC performs the communication at the 13.56 MHz frequency band with the RFID [1-3]. And a NFC-equipped device that supports following three modes : Initiator, Target, and Reader/Writer. And it may support Card Emulator[4]. Therefore, active communication is possible mutually.

III. Proposed NFC-based Forgery Prevention Method

NFC-based Forgery Prevention Method that is proposed in our paper is divided into the pre-registration, user registration and authentication process. Firstly, the description of used the terms in our proposed method is same as follows.

TABLE 1
Terminology

Symbol	Description
OG	Original Goods
SN	Secret Number
AuC	Certification Authority(Server)
E( )	Encryption
H( )	Hash Function
||	Concatenation
Puk	Public Key
prk	Private Key
T_{ID}	Unique Identification Number of Tag
P_{ID}	Unique Identification Number of Product
P_{NAME}	Product Name
P_{DATE}	Production Date
P_{CODE}	Producer code
P_{SLAN}	Provider Sign

Our proposed method includes a product(Luxury Goods), Smart Device(Phone) enabled NFC, as following Fig.1

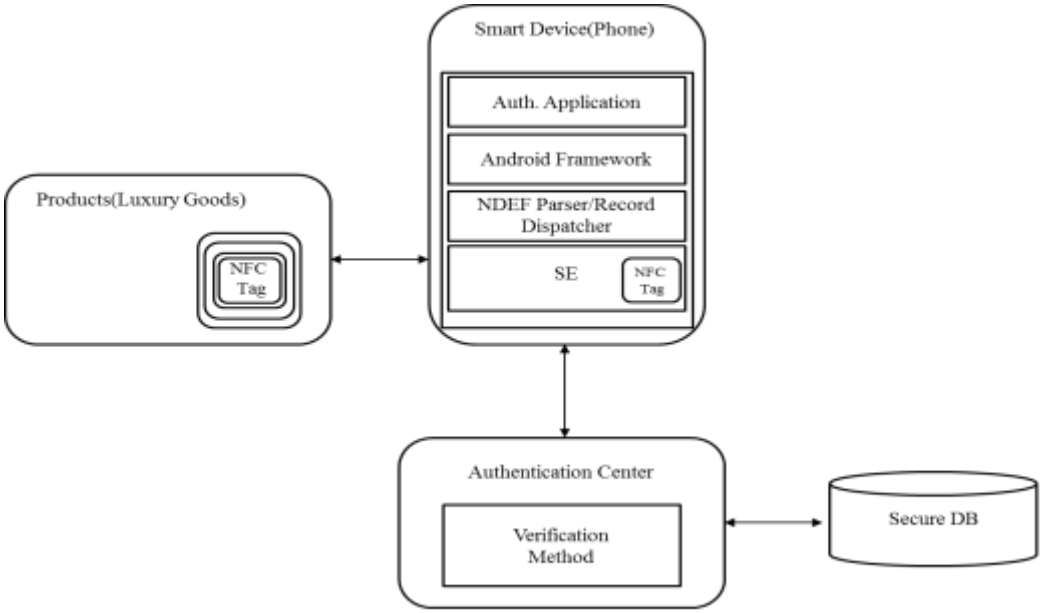

Fig.1 Architecture of the Authentication System

A. *Pre-Registration Phases*

This phase is performed before the product is shipped from the manufacturer. Firstly, manufacture writes various information like as P_{ID}, P_{NAME}, P_{DATE}, P_{CODE} and P_{SLAN}. And also store same data to server of AuC. And this time, this is registration state that it is performed by manufacture, thus rewriting is impossible(ROM MASK).

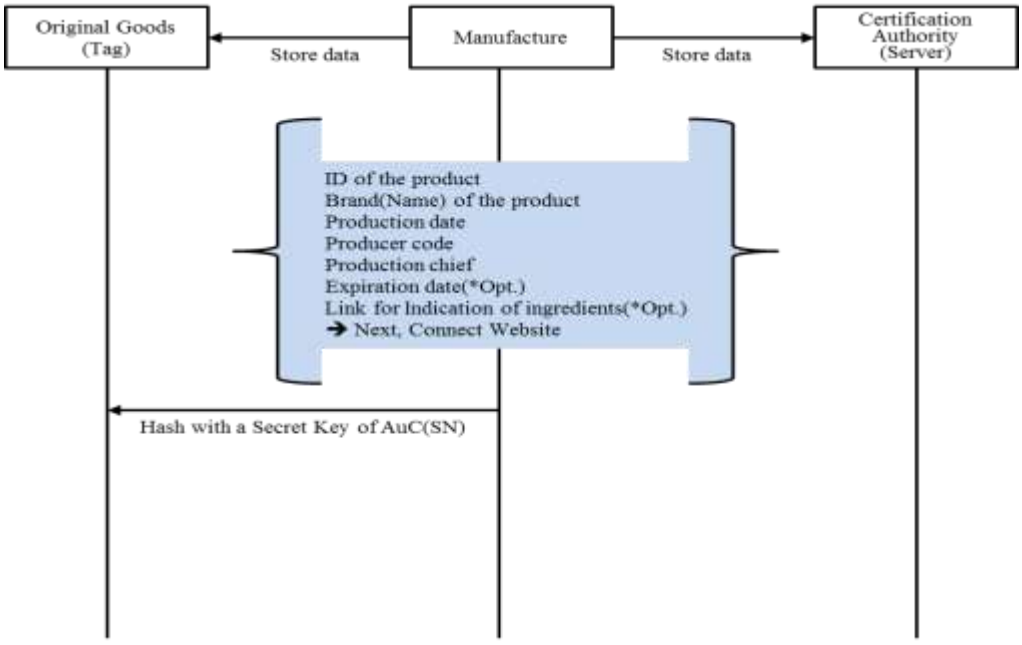

Fig.2 Pre-Registration Phase

B. User Registration Process

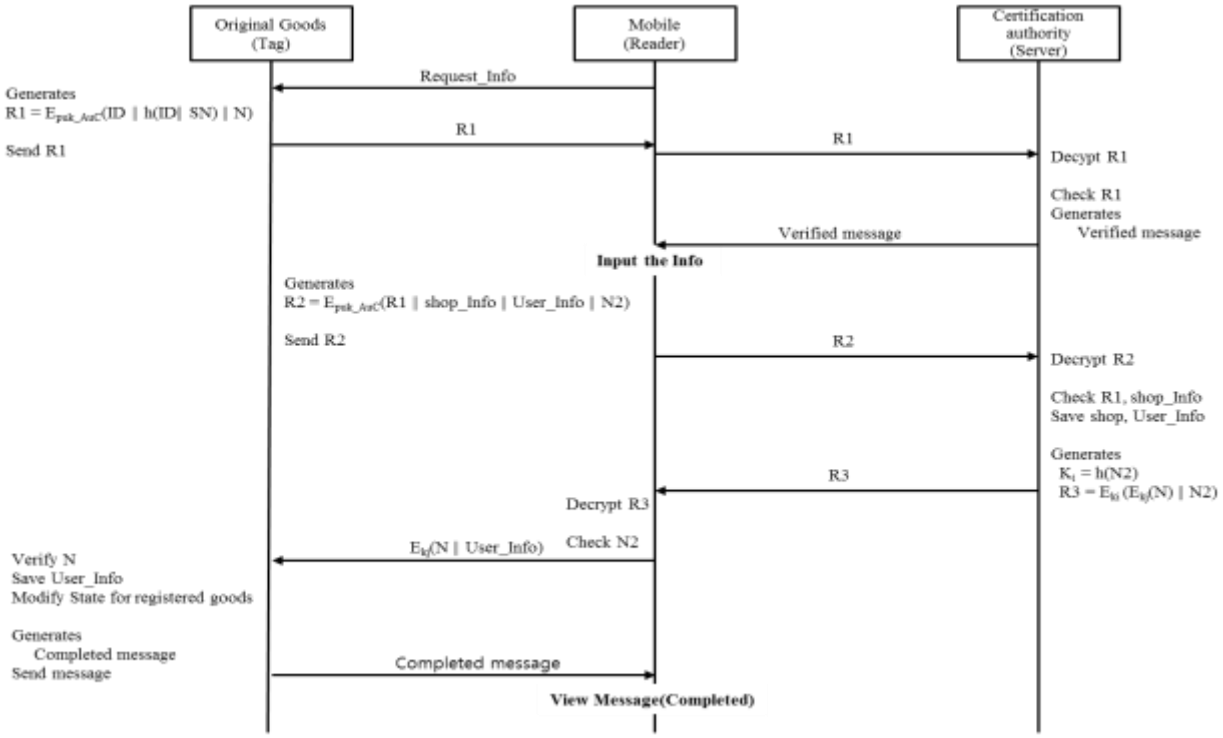

Fig.3 User Registration Process

This phase is processed when user purchases a product. The detailed step are as follows.

▪ Scenario and Registration Step

1. User tries to keep in touch with his mobile on the OG.
2. OG generates encrypted data R1 with nonce, SN of AuC and product ID using by public key of AuC. And sends R1 to mobile.
3. Mobile also sends R1 to AuC directly
4. AuC decrypts R1. And generates verified message, after checking the R1. And then, sends generated message to mobile.
5. Mobile display the result message.
6. Person who shop manager inputs the user and shop information through the App. And then, mobile encrypts the information of the product, shop and user with a nonce using by public key of AuC. And sends to AuC the generated message R2.
7. AuC checks R1(product ID), information of shop and user, after decrypting the R2. Make sure whether it stores in DB. And if verified, stores information of shop and user in DB.
8. Finally, generates R3 after generating key by nonce of mobile. Sends R3 to mobile.
9. Mobile decrypts the R3 using by public key of AuC. And then, checks generated a nonce value N2. Sends encrypted message with a nonce N and user information to OG.
10. OG stores user information, after verifying the nonce value N. And modify state information as a registration finished product. Finally, sends it to mobile, after generating the completed message.
11. Mobile shows message it has been completed the registration.

C. Authentication Process

This phase is final process in our proposed method. And substantially, this is a step to verify the validity of the product. Through stored information in server of AuC, to perform the verify about the product whether real or not. The detailed authentication processes are same as following.

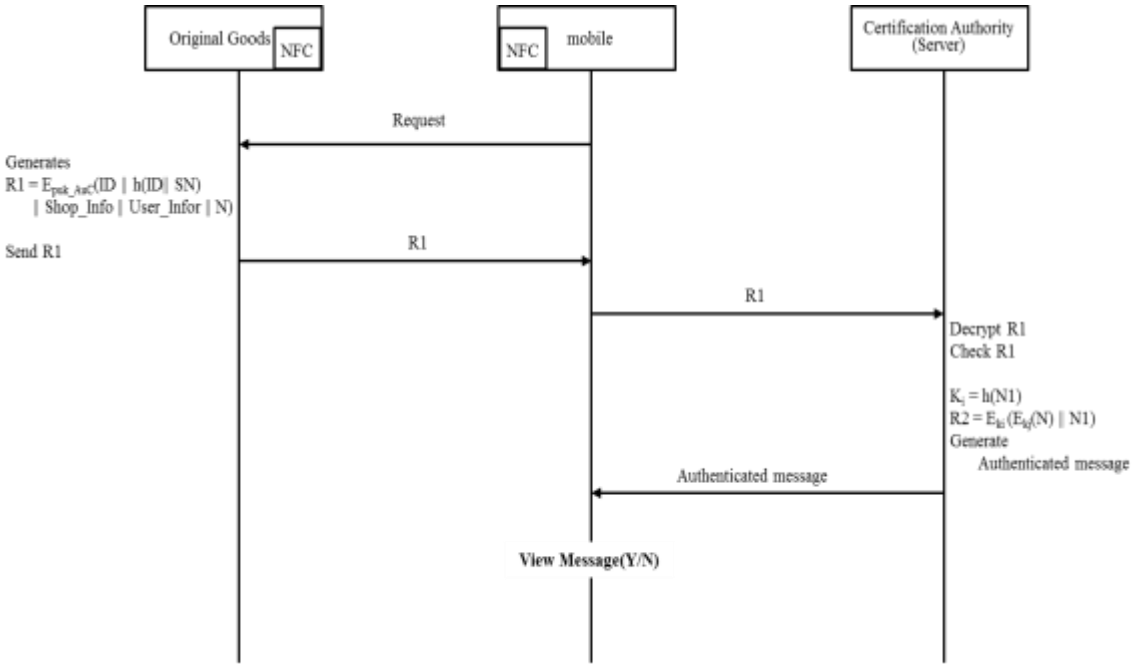

Fig.4 Authentication Process

▪ *Scenario and Authentication Step*

1. User tries to keep in touch with his mobile on the OG.
2. OG encrypts like as product ID, hashed message with a product ID and secure number SN of AuC, shop and user information, etc. using by a public key of AuC. Thus, R1 is made and sent to mobile.
3. Mobile sends received data R1 to AuC.
4. AuC checks R1, after decrypting the R1 by own private key. AuC can get information of the product, shop and user. And then, verifies storing above data in DB. And finally sends it, after generating the message it has been completed the authentication.
5. Mobile shows message by own screen.

IV. Conclusion

Our proposed authentication method for a forgery prevention can provide convenience to user. Because, user can directly access to product information using only a user's NFC-equipped smart phone. And because authentication information is stored in physically strong USIM file system, it can be stored and managed. Therefore, we propose an efficient NFC-based a forgery prevention method. Next, we will also process with the actual application and study based on this method.

Acknowledgment

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(2012R1A1B6002354).

This research was financially supported by the Ministry of Education, Science Technology (MEST) and National Research Foundation of Korea(NRF) through the Human Resource Training Project for Regional Innovation

References

[1] F. Michahelles, F. Thiesse, A. Schmidt and J.R Williams, "Pervasive RFID and Near Field Communication Technology," *IEEE Pervasive Computing*, Vol.6, No.3, 2007.
[2] M. Hutter and R. Toegl, "A Trusted Platform Module for Near Field Communication," in *Conf. Rec. 2010 ICSNC Conf*, France.
[3] H. C. Cheng, W. W. Liao, T. Y. Chi and S. Y. Wei, "A Secure and Practical Key Management Mechanism for NFC Read-Write Mode," in *Proc. 13th ICACT Conf*, Korea, 2011.
[4] NFC Activity Specification, NFCForum-TS-Activity-1.0, 2010.
[5] Eun Kim, Yun Seok Lee, Min Soo Jung, "Design and Implementation of an Authentication System for Anti-Forgery using the Smart Card," Journal of Korea Multimedia Society, Vol.14, No.2, pp.249-257, Feb.2011.
[6] ISO 18092 (ECMA-340). Information technology - Telecommunications and information exchange between systems - Near Field Communication - Interface and Protocol (NFCIP-1). Int. Organization for Standardization, Geneva, 2004.
[7] Moblie Near Field Communication (Mobile NFC) Stepping Stones, Version 1.0.0, SIMalliance, pp.10-15, (http://www.simalliance.org).
[8] Hasoo Eun, Hoonjung Lee, Heekuck Oh, "Conditional Privacy Preserving Security Protocol for NFC Applications, " ConsumerElectronics, IEEE Transactions on , vol.59, no.1, Feb. 2013.

Eun Kim received the B.S and M.S. degree in computer engineering from Kyungnam University, Changwon, Korea, in 2009, 2011. She will receive PH.D in Feb. 2015. Her research interests include Java Card, Security, Authentication and Secure Protocol.

Su Jin Lee received the B.S and M.S. degree in computer engineering from Kyungnam University, Changwon, Korea, in 1998, 2000. She is working on a PH.D. Her research interests include Java Technology, Network Security.

Hyun Joo Yoo received the B.S and M.S. degree in computer engineering from Kyungnam University, Changwon, Korea, in 1998, 2002. She is working on a PH.D. Her research interests include NFC, Mobile Payment Security, Mobile Platform Programming.

Jung Won Choi received the B.S degree in computer engineering from Kyungnam University, Changwon, Korea, in 2013. He will receive M.S degree in Feb.2015.

Seong Jeen Kim (S. J. Kim) received the B. S. degree, the M.S. degree and the Ph.D. in electrical engineering from Korea University in Seoul, Korea, in 1983, 1985 and 1993, respectively. For a while, he had studied in the Department of Electrical Engineering and Computer Science, University of Michigan, in An Arbor toward Ph. D degree from 1988.Since 1994, he has worked as professor in the Department of Electronic Engineering, Kyungnam University in Korea. His research interests are in the areas of semiconductor materials and devices , especially related to sensors.

Min Soo Jung received the B.S degree in computer engineering from Seoul National University, Seoul, Korea, in 1986. And he received the M.S degree and the PH.D in electrical engineering from KIST(Korea Advanced Institute of Science and Technology)in 1988, 1994. Since 1990, he has worked as professor in the Department of Computer Engineering, Kyungnam University in Korea. His research interests include Java Technology, Java Machine, Tag Technologies related to Electroic Payment.