Anti-counterfeit Ownership Transfer Protocol for Low Cost RFID System

CHIN-LING CHEN[1,*], YU-YI CHEN[2], YU-CHENG HUANG[1], CHEN-SHEN LIU[3], CHIA-I LIN[3] and TZAY-FARN SHIH[1]

[1]Department of Computer Science and Information Engineering
Chaoyang University of Technology, Taichung, 41349 TAIWAN (R.O.C.)
E-mail: {clc@mail.cyut.edu.tw; tidus.hinet@msa.hinet.net; tfshih@cyut.edu.tw}
[2]Department of Management Information Systems
National Chung Hsing University Taichung, 402 TAIWAN (R.O.C.)
E-mail: chenyuyi@nchu.edu.tw
[3]Innovative Supply-Chain Application Division Identification and Security Technology Center/
Industrial Technology Research Institute Hsinchu, 310 TAIWAN (R.O.C.)
E-mail: {CSLIU@itri.org.tw; Simon_Lin@itri.org.tw}

Abstract: Radio Frequency Identification (RFID) is a new technology. In recent years, it is convenient and feasible in many applications. However, it also addresses many security issues which are worth discussing. The Counterfeit imposes a menace to industry worldwide, and the problem is not specific for certain products or countries. In 2003, Koh et al. describe a RFID system based on "track and trace" solution to apply into pharmaceutical supply chain management to fight the counterfeit. Moreover, there are applications to solve malicious manner were presented. But there always still existed some disputes and not conform Class 1 Generation 2 (C1G2) standards. Unfortunately, the trick is changeable. The Koh et al.'s scheme is at premise rather primitive. In order to tackle this problem, we propose an anti-counterfeit ownership transfer protocol for low cost RFID system. We only use a tag to be a storage media. The proposed scheme can ensure a secure transaction.

Keywords: security; digital signature; authentication; Anti- counterfeit; ownership transfer; RFID; EPC

1 Introduction

Radio Frequency Identification (RFID) uses a mini equipment to store and receive remote information. The RFID system consists of the tags, readers, host, and antenna [1-13]. RFID tags can be broadly classified as two categories: those with a power supply and those without. RFID devices with power supply that actively transmitted to a reader are known as "active tags" and un-powered tags that are triggered by a reader are called "passive tags" .In every RFID object is a mini and low cost tag, receiving read-and-write message from the reader. The RFID reader sends a request signal, the tag will respond to it. The Electronic Product Code [14] lies in the tag to provide a unique code of the global product.

In 2003, Koh et al. [5] describe a RFID system based on "track and trace" solution to apply into pharmaceutical supply chain management to fight the counterfeit. The approach is sufficient in many cases, but in L. Batina et al. [15] pointed out that the used of RFID as an anti-countfeiting technology in Koh et al.'s scheme is at premise rather primitive.

It is deserved to be mentioned that the current RFID tag of low cost isn't a "Smart Tag" in generally. Most of that is just for storage or transmission. It's impossible to process complex computation on the current RFID tag. Therefore, it's just to be lightweight operations by wireless access [16-18]. It's irrational that assumed any information on the RFID tag would not be copied or stolen. In other words, there's a problem of the contention of

* *Corresponding author* (*E-mail address: clc@mail.cyut.edu.tw*)

the past researches [19-21], they all hold this contention and presume tag can capable secure and anti-counterfeit attacks by integrating digital signature [22] in their scheme. It is not a practical concept.

Actually, the above anti-counterfeit designs which directly write the digital signature into the RFID tag, and identify the digital signature can not perform anti-counterfeit function. Here we point out the critical problem is that only use the digital signature can not achieve the anti-counterfeit function. We review past literatures [23-27] proposed about ownership transfer concept, but these literatures basically still use the symmetric key cryptographic function, hash function and PKC (Public Key Cryptography) method, and regard the RFID tag to be a "Smart Tag". Because the current RFID tag's logic gates are about 500-5000, it's impossible to perform complex computations on the current RFID tags.

The current RFID standard ratified by EPCglobal is named EPCglobal Class 1 Gen 2 (Gen-2) RFID specification. We briefly summarize properties of Gen-2 RFID tag as follows [28]:

(1)Gen-2 RFID tag is passive, meaning that it receives power supply from readers.
(2)Gen-2 RFID tag communicates at UHF band (800-960 MHz) and its communication range is from 2 to 10 m.
(3)Gen-2 RFID tag supports on-chip Pseudo-Random Number Generator (PRNG) and Cyclic Redundancy Code (CRC) computation.
(4)Gen-2 RFID's privacy protection mechanism is to make the tag permanently unusable once it receives the kill command with a valid 32-bit kill PIN.
(5)Read/Write to Gen-2 RFID tag's memory is allowed only after it is in secure mode.

Due to the current RFID tag is just a storage media which accesses via wireless and the computing resource was limited. Therefore, there exits an insecure crisis, the intruder just need to carry a mobile reader and send a request information to a tag, tag will response information and signature to the reader, so the intruder will obtain the original signature easily. Continuously, the dummy-OEM only need to write the stolen signature into the RFID tag of any counterfeit product, and the intruder can forward these counterfeit products to the commercial agent for sale which is regarded as the legal products. Once the consumer purchases the product and asks to verify its validity, the reader of commercial agent will send a read request aim at the RFID tag on the product, the RFID tag will respond signature to the reader of commercial agent. Due to the stolen original signature has been written into the RFID tag, thus the commercial agent also can prove its correctness to the consumer. The scenarios are illustrated as Fig. 1.

In fact, the digital signature is used to be verified by anyone. However if such concept be applied to anti-counterfeit design, and anyone can duplicate the signature and relevant information from the RFID tag, and then store on another RFID tag. The false tags which with copies the legal signature can also pass the identification. That is only with signature mechanism can not perform anti-counterfeit. Thus, we propose a novel anti-counterfeit ownership transfer protocol for RFID system with efficient and lightweight computation via online authentication.

The proposed protocol should possess an online authentication and has the following requirements:

(1) Against attacks (such as replay attack, man-in-the-middle attack etc.).
(2) Anti-counterfeit (Prevent a great deal of tag's clone)
(3) Lightweight computation and conform C1G2 standards.
(4) With ownership transfer.

The other sections of the paper are as follow: the proposed protocol content will be involved in section 2. We also analyze the requirements in section 3, and make a conclusion in section 4.

2 Our Scheme

Our scheme divides into three phases: (1) Initialization phase (2) Purchase Phase (3) Ownership transfer phase. The brief scenarios are illustrated in Fig.2.

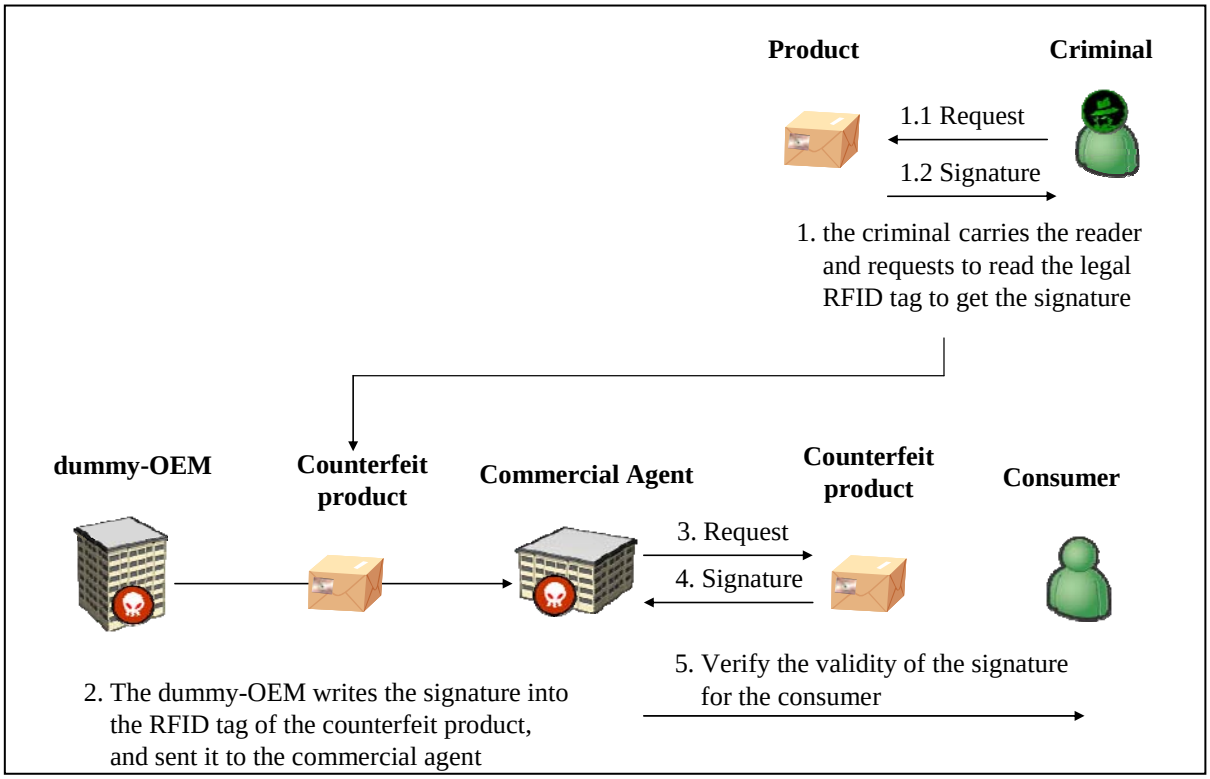

Fig. 1. The scenarios of the illegal behavior under the interception

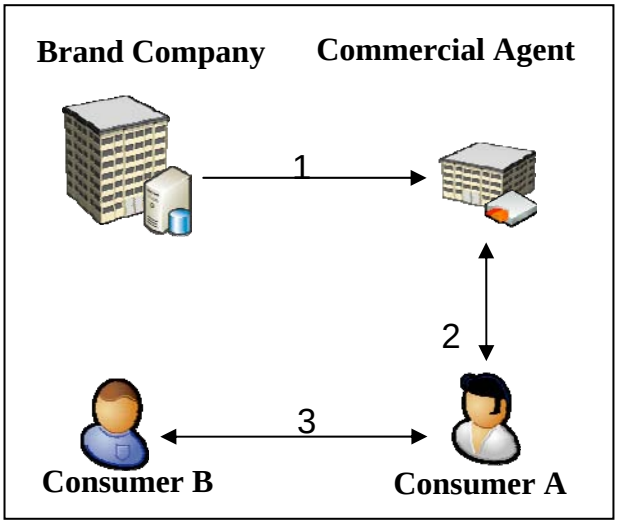

Fig. 2. The brief scenarios of our scheme

Step 1 : The product with RFID tag is sent to commercial agent by various channels.
Step 2 : The consumer A wants to buy the product and verify the product.
Step 3 : The consumer B confirms to purchase the product of consumer A. The consumer A transfers the ownership to the consumer B.

2.1 Notation

M_{reg} : the request message.
PK_X : X's public key.
SK_X : X's private key.
PW : the consumer's password.
PW_{NEW} : the new consumer's password.
EPC_X : Electronic Product Code of a tag X.
ID_X : the identity of X .
$Cert_X$: the certificate of the object; when user purchases the object X, he has the certificate $Cert_X$.
$V_X(m)$: use X's public key to verify the message m.
$S_X(m)$: use X's private key to make the signature of the message m.
$H(\cdot)$: one way hash function.
SN : the serial number of the product.
Msg : a confirmation message for confirming a transaction.
Key_T : an authorized key, when reader

wants to write data into tag. The reader needs the authorized key Key_T .

SG ： the signature of the brand company.

$A \overset{?}{=} B$: compare whether A is equal to B or not.

||: concatenation operation.

2.2 Initialization Phase

Suppose the OEM (Original Equipment Manufactures), the commercial agent and the authorized agent's reader obtain the certificates from brand company via online authentication to verify if the communication correctly with the end server in advance.

The Secure Socket Layer (SSL) channel is built between the brand company and commercial agent in advance. The identification of each reader and server depends on the secure channel of the PKI (Public Key Infrastructure).

Therefore, the brand company authorized the OEM to manufacture new products. The OEM will read the ID_T via the authorized reader which sending the information of the product to the brand company to get a unique EPC, serial number, digital signature and the authorized key Key_T. The information will also be recorded in the server database.

Simultaneously, the OEM gets the authorized key Key_T, it will use the Key_T to write *SN*, *EPC*, digital signature into the product tag. The tag stored the product information (ID_T, EPC_T, *SN*, SG_T). Finally, the product will be sent to the authorized commercial agent.

2.3 The Purchase Phase

In this phase, we describe the consumer how to buy the product from commercial agent, and the consumer how to identify the counterfeit products.

Firstly, commercial agent's reader makes an off-line authentication with the RFID tag, and shows the verification result to consumer. Once the consumer confirms to purchase the product, the commercial agent will ask the consumer to enter a password, and then the commercial agent will forward the hash value of password to the brand company's server for registration.

The brand company's server will regenerate a new signature SG_T' and a new serial number *SN*' for the RFID tag. The database will update and send related information including the authorized key Key_T to the commercial agent. The commercial agent's reader uses the authorized key Key_T to write the new signature and new serial number into the tag.

2.4 Ownership Transfer Phase

If the consumer A wants to sell and transfer the ownership of the products to consumer B, he can go to the authorized neighborhood site (authorized agent) to show B whether the product is original or not via the backend server sent back the message *Msg*. If the *Msg* is the same as the original one, the consumer B only trusts reader of this authorized agent.

Therefore, the consumer A enters the self-setting password *PW*, and then the consumer B enters a new password $PW_{new,}$. The two passwords are calculated by one way hash function will transfer to the brand company server for authentication.

After calculating the hash value of consumer B's password, the new signature value will be sent back to the brand company server for generating a set of new signature, new serial number and identification message *Msg*. They will be transmitted to the authorized agent's reader.

Finally, the reader writes the new signature and serial number to the RFID tag by using the authorized key Key_T, and then prints the identification message *Msg*. The Fig. 3 shows the flow chart of the ownership transfer phase.

Step 1：The reader sends a request message M_{reg} to the tag.

Step 2：Upon receiving the M_{reg}, the tag will transfer the stored (ID_T, EPC_T, SN, SG_T) to the reader.

Step 3：The reader will use the server's public key to verify the correction of the SG_T as follows:

$$V_s(SG_T) \overset{?}{=} H(ID_T \,||\, EPC_T \,||\, SN) \quad (1)$$

If it is correct, the reader will use its own private key to make the signature of the message $(H(ID_R, ID_T, SG_T))$

$$S_1 = S_R(H(ID_R, ID_T, SG_T)) \quad (2)$$

The reader transfers $(ID_R, ID_T, S_1, SG_T, Cert_R)$ to the server.

Step 4：After receiving the above message, the server will use the reader's public key to verify $Cert_R$. If the verification is correct, the server will use the reader's public key to verify the correction of S_1 as follows:

$$V_R(S_1) \stackrel{?}{=} H(ID_R, ID_T, SG_T) \quad (3)$$

If the verification is correct, check whether ID_R in database equals to the received ID_R ; if it is correct, then pick out the EPC_T and the SN of the ID_T in the database. The server will use its own public key to verify the correction of SG_T as follows:

$$V_S(SG_T) \stackrel{?}{=} H(EPC_T \,||\, SN) \quad (4)$$

If the verification is correct, then pick out the *Msg* in the database, and the server uses its own private key to make the signature of the message $H(Msg)$ as follows:

$$S_2 = S_S(H(Msg)) \quad (5)$$

The server will transmit the message (Msg, S_2) to the reader.

Step 5：The reader will use the server's public key to verify the correction of S_2 as follows:

$$V_S(S_2) \stackrel{?}{=} H(Msg) \quad (6)$$

If the verification is correct, consumer A (the old owner of the product) enters *PW* choice himself at buying time and generates a hash value *H*(*PW*), the consumer B (the new owner of the product) enters new password PW_{new} and generates a hash value $H(PW_{new})$, and the reader uses its own private key to make the signature of the message $(H(H(PW), H(PW_{new})))$ as follows:

$$S_3 = S_R(H(H(PW), H(PW_{new}))) \quad (7)$$

After that, the authorized reader will transmit the message $(H(PW), S_3)$ to the server.

Step 6：The reader will use the server's public key to verify the correction of S_3 as follows:

$$V_R(S_3) \stackrel{?}{=} H(H(PW), H(PW_{NEW})) \quad (8)$$

If the verification is correct, check if *H* (*PW*) of the ID_T in database equals the received *H(PW)*, and check the Key_T of the ID_T in database. The server generate a new *SN*' and new *Msg*', and then update the record $(ID_T, ID_R, Key_T, Msg', SN', H(PW_{NEW}))$. The server will use its private key to make the signature of the message $H(EPC_T \,||\, SN')$ as follows:

$$SG_T' = S_S(H(EPC_T \,||\, SN')) \quad (9)$$

After that, the server will use its own private key to make the signature of the message $(H(Msg, Key_T, SN, SG_T))$ as follows:

$$S_4 = S_S(H(Msg, Key_T, SN, SG_T)) \quad (10)$$

The server will transmit the message $(Msg', Key_T, SN', SG_T', S_4)$ to the reader.

Step 7： The reader uses the server's public key to verify the correction of S_4 as follows:

$$V_S(S_4) \stackrel{?}{=} H(Msg', Key_T, SN', SG_T') \quad (11)$$

If the verification is correct, the reader prints the transaction receipt (includes *Msg*) for the consumer.

The reader uses the authorized key Key_T to write the serial number SN' $(SN = SN')$ and the tag's signature SG_T' $(SG_T = SG_T')$ into tag.

3 Analysis

In this section, we will examine whether the requirements mentioned in section one are satisfied or not.

3.1 Applied into Low Cost and the Limited Computing Resource Tag

Our proposed scheme can apply into the low cost and the limited computing resource tag. Due to the step 7 of the ownership transfer phase, the commercial agent's reader uses the authorized key Key_T to write the new serial SN' and new signature SG_T' into the tag. The tag is just only a storage media. It doesn't need any additional operations. Thus, it is suitable to current limited computing source tag.

3.2 The Tag Doesn't Need to Perform the Complex Operation and Increase Access Speed

The proposed scheme with the limited computing resource tag doesn't need to perform the complex operation. In step 2 and step 7 of the ownership transfer phase, the tag only need to store (ID_T, EPC_T, SN, SG_T) and update new serial

number SN' and new signature SG_T' .The tag doesn't need to perform the complex operation entirely. Thus, the access time can be decreased.

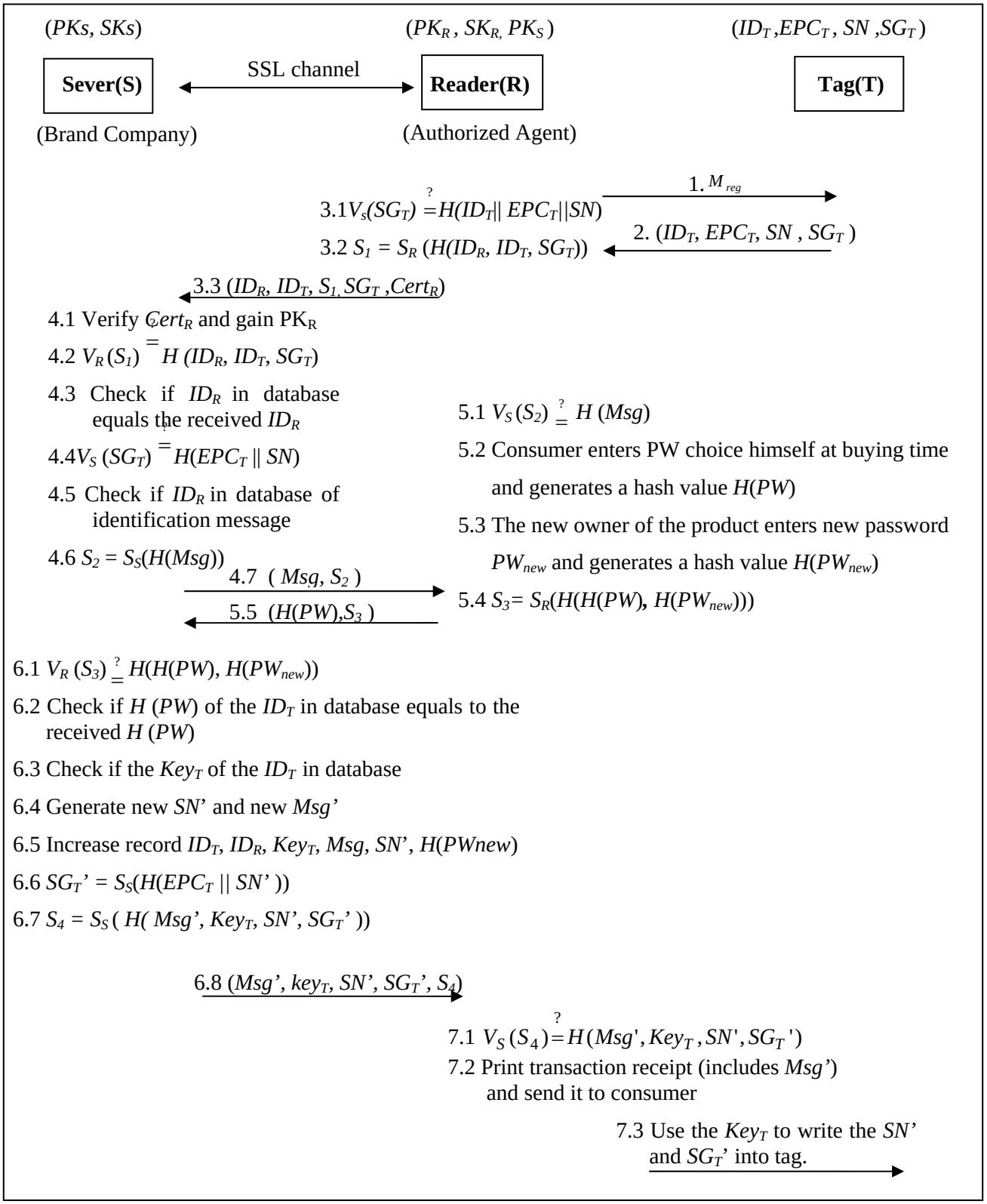

Fig. 3. The flow chart of the ownership transfer phase

3.3 Prevent a Great Deal of Tag's Clone

In aspect of preventing a great deal of tag's clone, our proposed scheme can prevent illegal clone. In step 7 of the ownership transfer phase, the verification function is shown as follows:

$$V_S(S_4) \stackrel{?}{=} H(Msg', Key_T, SN', SG_T') \quad (11)$$

The reader checks the correctness of the signature S_2 via online verification. If it is correct, the reader regenerates a set of serial number SN' and signature SG_T' and the reader use the authorized key Key_T to writes (SN', SG_T') into the tag to update serial number and signature for each transaction. Once the illegal clone occurs, the illegal behavior will be detected. In other words, if the attacker obtained (SN', SG_T'), but the attacker doesn't know the authorized key Key_T, so the attacker writes the correct (SN', SG_T') into the tag to update serial number and signature were impossible. Thus, our scheme can prevent from a great deal of tag's clone

3.4 Against Replay Attack

In the current world, the attacker may want to impersonate a legal signature to the reader. If the attack occurs, the behaviors of counterfeit may be dangerous. To prevent the latent danger, one-time signature is used in our scheme. The scheme can resist the replay attack. Due to the step 6 of ownership transfer phase, the server will regenerated a new *SN*', *Msg*' and SG_T' for each transaction, the server also made the signature S_i with a one-way hash function and its own private key. Thus the attacker can not spoof the reader by transmitting the obtained previous *SN* and SG_T to pass the authentication for this transaction.

3.5 Against Man-in-the-Middle Attack

In step 6 of the ownership transfer phase and, the server generates the new signature S_i' with one-way hash function and its own private key. Thus, attackers cannot forge a legal signature to pass the reader's authentication. On the other hand, it is easy to prove whether signature S_i is generated by the server. Due to the server regenerates the signature S_i with the new SG_T', SN' for each transaction. And the reader uses the authorized key Key_T to update the tag's signature SG_T' and serial number *SN'*. Therefore, Man-in-the-Middle attack can be prevented since the intruder has no knowledge of server's private key and the authorized key Key_T.

3.6 Conforming EPC Class 1 Generation 2 Standards

In our proposed protocol, the tag is just a storage media. For instance, the reader obtained signature and serial number from the server, and using authorized key Key_T to update signature and serial number without any complex computation. In other word, due to the capability-limited RFID tag doesn't need to make the complex operations (such as hash function, symmetric encryption/decryption, or asymmetric encryption encryption/decryption etc. operations) in our protocol. The proposed scheme can conform to EPC Class 1 Generation 2. standards.

3.7 With Ownership Transfer

In this paper, the purposed scheme can be applied to high price product for ownership transfer. In step 6 of the ownership transfer phase, when the consumer A (the old owner) enters *PW* chose himself at buying time and generates the hash value *H*(*PW*), the consumer B (the new owner) enters new password PW_{new} and generates the hash value $H(PW_{new})$. The reader uses its own private key to make the signature as follows:

$$S_3 = S_R(H(H(PW), H(PW_{new}))) \quad (7)$$

After that, the reader transmits the message $(H(PW), S_3)$ to the server. Upon receiving the message form server, the reader will use server's public key to verify the correction of S_3 as follows:

$$V_R(S_3) \stackrel{?}{=} H(H(PW), H(PW_{NEW})) \quad (8)$$

If the verification is correct, then check whether or not *H*(*PW*) of the ID_T in database equals to the received *H*(*PW*). The server regenerates *SN*' and SG_T' transfers the ownership to the owner B.

The authorized reader uses the authorized key Key_T to write the SN' and SG_T' into the tag. Thus, our scheme achieves the ownership transfer.

3.8 Comparison with Previous Schemes

We compare the security and property of the proposed method with those of the previous schemes in table 1. Due to the EPC C1G2 standards

only permit the simple operations (for example exclusive-OR, random number generation and CRC operations) for tags' operation. Some previous schemes often used the symmetric or asymmetric cryptosystem to implement their applications. These schemes do not conform the EPC C1G2 standards. Thus, they are not suitable to current low cost tag. Simultaneously, the proposed scheme can resist various attacks and with mutual authentication. None of the previous methods achieve all requirements, but the proposed method achieves all requirements.

4 Conclusion

At present, the cost of the RFID tag is still too high, in spite of many literatures are supposed that the RFID tag has sufficient computing resource. Due to the current tag are limited the logic gates, their proposals are impractical. Thus, how to add the anti-counterfeit mechanism to the passive RFID tag with low cost and limited computing resource is the emerging issue.

In this paper, we only use the passive RFID tag to be a storage media to propose a secure authentication transaction with ownership transfer. The proposed scheme not only with the online authentication but also meet the following requirements.

(1) Applied to low cost and the limited computing resource tag.
(2) The tag doesn't need to make the complex operation and increase access speed.
(3) Prevent a great deal of tag's clone.
(4) Against the replay attack.
(5) Against Man-in-the–Middle attack.
(6) Only simple computing operations (e.g. use exclusive-OR, Cyclic Redundancy Code and generate random number etc.) are applied to conform to EPC Global C1G2 standards.
(7) With ownership transfer.

We proposed an anti-counterfeit ownership transfer protocol such that against attacks, anti-counterfeit, and lightweight computation to conform the C1G2 standards requirements can be guaranteed. The tag only needs update new signature and new serial number. Thus the RFID tag doesn't need to make the complex computations

In the future, the online verification should be integrated with the EPC network. For all sale products, the users can verify whether or not the original and fake of the products.

Table 1. Comparison of the related schemes

Scheme / Property	Seo et al. [23]	Osaka et al. [24]	Koralalage et al. [26]	Fouladgar et al. [27]	Our scheme
Resist to Man-in-the–middle attacks	Yes	No	Yes	Yes	Yes
Resist to replay attack	Yes	Yes	Yes	Yes	Yes
Resist to DOS attack	Yes	Yes	No	Yes	Yes
GEN-2 conformation	No	No	No	No	Yes
Mutual authentication	No	No	No	Yes	Yes
Ownership transfer	Yes	Yes	Yes	Yes	Yes

References:

[1]S. L. Garfinkel, A. Juels, R. Pappu (2005), RFID Privacy: An Overview of Problems and Proposed Solutions, *IEEE Security & Privacy*, Vol. 3, No. 3, pp. 34-43.

[2]S. Srinivasan, Akshai Aggarwal, Anup Kumar, RFID Security and Privacy Concerns, *WSEAS Transaction on Communications*, Vol. 5, Feb. 2006, pp. 1109-2742.

[3] Lehtonen, M. O., Michahelles, F., and Fleisch, E. (2007), Trust and Security in RFID-Based Product Authentication Systems, *IEEE Systems Journal*, Vol. 1, No. 2, pp. 129-144.

[4] Potdar, M., Chang, E., and Potdar, V. (2006), Applications of RFID in Pharmaceutical Industry, *2006 IEEE International Conference on Industrial Technology* (ICIT 2006), pp. 2860-2865.

[5] R. Koh, E. W. Schuster, I. Chackrabarti, and A. Bellman (2003), Securing the Pharmaceutical Supply Chain. White Paper MIT-AUTOID-WH-021, Auto-Id Center MIT, Cambridge, Ma 02139-4307, USA. Available at http://www.mitdatacenter.org/MIT-AUTOID-WH021.pdf.

[6] Juhan Kim, Dooho Choi, Inseop Kim, and Howon Kim (2006), Product Authentication Service of Consumer's mobile RFID Device, *2006 IEEE Tenth International Symposium on Consumer Electronics* (ISCE '06), pp.1-6.

[7] Juhan Kim, Dooho Choi, Inseop Kim, and Howon Kim (2006), Product specific security features based on RFID technology, 2006 *International Symposium on Applications and the Internet Workshops*, (SAINT Workshops 2006), Page(s):4.

[8]S. F. Wamba, L. A. Lefebvre, Y. Bendavid and É. Lefebvre (2008), Exploring the impact of RFID technology and the EPC network on mobile B2B eCommerce: A case study in the retail industry, *International Journal of Production Economics*, Vol. 112, No. 2, pp. 614-629.

[9]E. Bottani and A. Rizzi (2008), Economical assessment of the impact of RFID technology and EPC system on the fast-moving consumer goods supply chain, *International Journal of Production Economics*, Vol. 112, No. 2, pp. 548-569.

[10]Shu-Jen Wang, Shih-Fei Liu and Wei-Ling Wang (2008), The simulated impact of RFID-enabled supply chain on pull-based inventory replenishment in TFT-LCD industry, *International Journal of Production Economics*, Vol. 112, No. 2, pp.570-586.

[11]P. Vrba, F. Macůrek and V. Mařík (2008), Using radio frequency identification in agent-based control systems for industrial applications, *Engineering Applications of Artificial Intelligence*, Vol. 21, No. 3, pp. 331-342.

[12]L.C Wang (2008), Enhancing construction quality inspection and management using RFID technology, *Automation in Construction*, Vol. 17, No. 4, pp. 467-479.

[13] King, Brian and Zhang, Xiaolan (2007), Securing the Pharmaceutical Supply Chain using RFID, *2007 International Conference on Multimedia and Ubiquitous Engineering (MUE '07)*, pp. 23-28.

[14]EPC (Electronic Product Code) Class 1 Generation 2 standards by EPCglobal, web site: http://www.epcglobalinc.org/

[15] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede (2007), Public-Key Cryptography for RFID-Tags, 2007 F*ifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops '07)*, pp.217-222.

[16]H. Y. Chien, C. H. Chen (2007), Mutual authentication protocol for RFID conforming to EPC class 1 generation 2 standards, *computer standards & interfaces*, Vol. 29, No. 2, pp.254-259.

[17]C. L. Chen and Y. Y. Deng, A practical RFID system: with mutual authentication and privacy protection, *2007 Taiwan Academic Network Conference, (TANET2007)*, Taiwan Taipei (Taiwan university), Oct., 2007, pp.25-27.

[18]Valdis Pornieks, Egils Ginters, Security Problems of RFID Authentication Protocols, *the WSEAS International Conference on System Science and Simulation in Engineering (ICOSSSE '07)*, Nov. 2007. Venice, Italy.

[19]T. Staake, F. Thiesse, and E. Fleisch, Extending the EPC network: The potential of RFID in anti-counterfeiting, *20th ACM Symp. On Applied Computing*, Santa Fe, NM, Mar. 2005, pp.1607-1612

[20]M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, Strong authentication for RFID systems using the AES algorithm, *Cryptographic Hardware and Embedded Systems*, Boston, MA, 2004, pp. 357-370.

[21] Yung-Chin Chen, Wei-Lin Wang, and Min-Shiang Hwang (2007), RFID Authentication Protocol for Anti-Counterfeiting and Privacy Protection, *The 9th International Conference on*

Advanced Communication Technology, Vol.1, pp. 255-259.

[22]Joseph K. Liu, Karyin Fung, Duncan S. Wong, Providing High Availability to Time-Stamping Services Using Threshold Signature, *WSEAS Transaction on Communications*, Vol. 3, No. 1109-2742. April 2004.

[23]Y. Seo, T. Asano, H. Lee, and K. Kim, A Lightweight Protocol Enabling Ownership Transfer and Granular Data Access of RFID Tags, *the 2007 Symposium on Cryptography and Information Security Sasebo*, Japan, Jan. 2007, pp. 23-26.

[24]K. Osaka, T. Takagi, K. Yamazaki, and O. Takahashi, An Efficient and Secure RFID Security Method with Ownership Transfer, *IEEE International Conference on Computational Intelligence and Security*, Japan. Vol. 2, Nov. 2006, pp. 1090-1095.

[25]M. David, S. Andrea, and W. David, A Scalable, Delegatable Pseudonym Protocol Enabling Ownership Transfer of RFID Tags, *Selected Areas in Cryptography – SAC 2005*, *Lecture Notes in Computer Science (LNCS 3897)*, Springer-Verlag, Kingston, Canada, Aug. 2005, pp. 276-290.

[26]K.H.S. Sabaragamu Koralalage, S. Mohammed Reza, J. Miura, Y. Goto, and J. Cheng, An Approach to Enhance the Security and Privacy of RFID Systems Used in Product Lifecycle with an Anonymous Ownership Transferring Mechanism, *Proceedings of the 2007 ACM symposium on Applied computing*, Mar. 2007, pp. 270 – 275.

[27] Sepideh Fouladgar, Hossam Afifi, A Simple Privacy Protecting Scheme Enabling Delegation and Ownership Transfer for RFID Tags, *Journal of communications*, Vol. 2, No. 6, Nov. 2007.

[28]EPCglobal Inc., Class 1 Generation 2 UHF Air Interface Protocol Standard Version 1.09", Available web site: *http://www.epcglobalinc.org/standards/technology/specifications.html*.