Based on RFID Products Information Tracing Anti-counterfeiting Strategy Design and Application

JIAO YABING

Shandong Yingcai University,
Jinan, Shandong ,China

Abstract:

Research one security policy in the INTERNET GSM or other possible environments based on the uniqueness and uniformity of RFID chips code and EPC. Its basic process: the data in RFID chips—products database—verification. Its technological process: the READER reads encrypted data in RFID chips some kind of products corresponding and uploads the data to public networks. The EPC database on line returns user verification after data processing. According to the strategy of anti-counterfeiting technology, the introduction of PKI technology on digital certificate management, system describes the digital certificate application and verification process. Finally, the introduction of the hash algorithm, design implementation process RFID tag-based anti-counterfeiting, and various algorithms and comparative analysis of tags, readers secure communications mechanism.

Keywords: *radio frequency identification; security policy; guarding against fakes; Public Key Infrastructure; hash algorithm*

Introduction

As a kind of new technology, the technology of radio frequency identification (RFID) has been applied widely to the management of products information, and become apparent visible economic benefit because of its characteristic of untouched and auto-read-write[1] [2]. At the same time, the compatibility between RFID data read-write and other information system makes RFID take on powerful life-force in the dynamic products management. Compared to the bar-code technology and laser technology the RFID have a great lot of strongpoint. For example, its tags can store much more information, work under the terrible circumstance and RFID can be used in electron information system to achieve safely products information retrospecting [3]. Because of above mentioned strongpoint, security policy of products information retrospecting based on RFID technology and building a kind of system of products information ietrospecting must offer a new occasion for the breakthrough of security policy of products.

2. Security characteristic of RFID

RFID system includes three parts: Tag, reader and antenna. Tag is made up of coupling element and chip. Every tag has one and only electron code; Reader is used to read or write the products electron information for tags; Antenna is an element between tags and reader to transfer the radio frequency signal [1]. The most important RFID advantage compared with laser security technology or bar-code technology is that every tag has one and only ID on the earth. Namely, the serial number alone is encapsulated in the chip's memory of every tag when the tag was turn out and not altered.

When we undergo affirming some products real or bogus, the accredited device can help us to read out the information encapsulated in these RFID tags throughout INTERNET, Global System for Mobile

communication (GSM) which makes corporation information open but safe via ERP or other corporation management information system (MIS). In this process, the other third party could not copy the serial number alone is encapsulated in the chip's memory of every tag. The base data stream process is just as Fig.1.

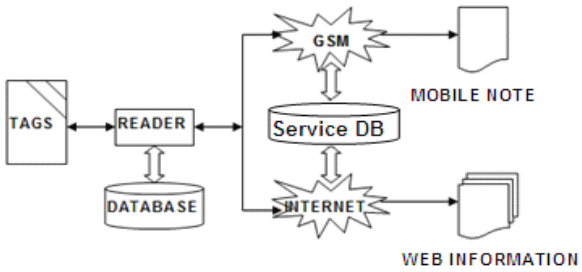

Fig. 2 Model of Security Policy of Products Information Retrospecting

Fig. 1 Process of RFID Data Reading and Feedback

3. Security project of products information retrospecting based RFID

Why RFID technology is used to guarding against fakes is because that its data functions: writing, transmission, getting, dealing with. In this process the data information in RFID chip attached product may go for many different kinds of public MIS.

3.1 Building of the security policy model of based on RFID

Because the data digital code in RFID and electronic products code (EPC) is one and only and accordant, the research may verify some a product fake or not though the public plat just like INTERNET or GSM by comparing the two sets of codes. The basic process: RFID data in chip——product database——verification. The principle flow: RFID reader reads the tag chip data encrypted comparing to some a kind of product, then transmits this data to the public network; The data is decoded by MIS base on the database of the public service plat or EPC; The MIS feeds back product user or official checkout organization one set of information verified[4]. The follow Fig.2 shows us this process.

3.2 The key technology of security policy based on RFID

The given security policy based on RFID is based upon the technology of digital underwriting and the characteristic of serial ID enveloped in product RFID tag, unique and immutable. The care process includes two parts: enveloping digital underwriting, reading and decrypting the information in the RFID tag. In the process digital information enveloped, we deal with the digital certificate attached some one kind of product and the serial ID preparing to writing in RFID tag, then gain a digital abstract. In this process, the producers use their private key encrypt the digital abstract. In the end, the unique digital underwriting is given. The digital underwriting will be read in RFID tag according with its digital certificate. The second process is to verify on line. In this process the digital underwriting may be decrypted on public network just comparing to the first process product information enveloped. Above two processes are based upon MIS and public network. When the MIS finished data dealing the digital abstract and ID will be re-gain. The consumer may compare the digital abstract and ID above-mentioned with the paper digital certificate information attached product and the serial ID printed on the product pack to verify their goods true or not. The Fig.3 show us whole process.

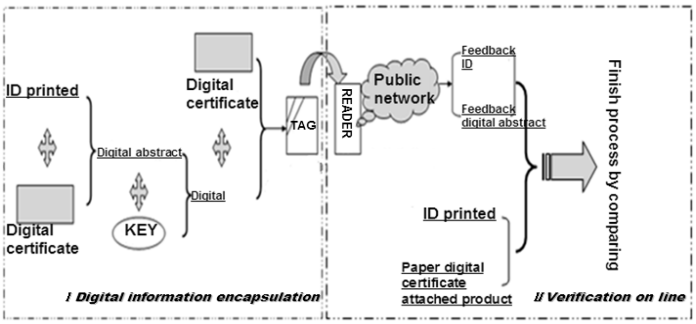

Fig. 3 Technological Process of Security Policy

4. Digital certificate application process

The system used PKI(Public Key Infrastructure) technology on the tag digital certificate management.PKI [21-23] refers to the use of public key concepts and techniques, the implementation of the provide universal security services infrastructure.In the X.509 standard, in order to distinguish it from the Privilege Management Infrastructure, defines the PKI to support public key management and support authentication, encryption, integrity and accountability services infrastructure.The complete PKI system must have the Certificate Authority, library of digital certificates, key backup and recovery system, certificate void the basic components of the system, application programming interface(API).

4.1. PKI System Components

1)Certificate Authority

CA was responsible for the admissibility of the digital certificate request and issuing .CA must have authoritative features, is a trusted third party.

2) PKI database

PKI database used to manage the storage has been issued a digital certificate and a public key, the user can thereby obtain the required other user's certificate and public key.

3)Key Management Center

Review checklist and other key management issue has not been canceled, abnormal key for key life cycle process.

4)Key backup and recovery system

If the user lose the key used to decrypt the data, the data would not be able to be decrypted, which will cause loss of valid data. To avoid this situation, PKI key backup and recovery mechanisms. Key backup and recovery must be done by a trusted third party to. And key backup and recovery only for the decryption key, the signature private key to ensure its uniqueness without backup.

5)Certificate void system

Record the certificate void system is responsible for the voided certificates of expired certificates or other reasons responsible for the recovery, the certificate needs to be recorded, to retain the certificate is no longer repeated issuance.

6) application programming interface

Provide a good interface system makes a wide variety of applications can be a safe, consistent, credible and PKI systems interact to ensure the integrity and ease of use of a secure network environment.

4.2. Digital certificate application process

The concrete steps are as follows

1 Tag production enterprises to the PKI apply for a digital certificate, PKI system to the user to create a bunch of random code, this string of code is the digital certificate invitation code PKI will match string code and the legitimate domain name store PKI database.

2 PKI management department code via a secure manner distributed enterprises, such as encrypted messages.

3 Enterprises to obtain a digital certificate invitation code, login the PKI certificate application page, submit a completely legitimate domain names and digital

certificates invitation code to PKI system will issue a digital certificate request

4 invitation code PKI system detects a fully qualified domain name corresponding digital certificates are submitted to the system certificate application invitation code consistent response certificate issued, the data of the certificate issued to enterprises through legitimate channels, or will refuse the certificate was issued.

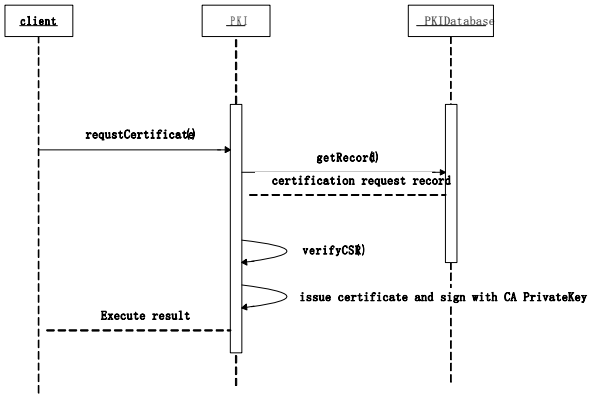

Fig . 4 Client request certificate from PKI

4.3 The complete certificate validation process

User or service terminal to the PKI submit a digital certificate authentication request, the certificate PKI public key encryption.

Receives an authentication request to PKI data using its own private key to decrypt operation get certificate plaintext.

Contrast certificate information system user's original certificate of the certificate issued to see if it is expired or the presence of other abnormalities. Answering user to submit a certificate application for certification requests.

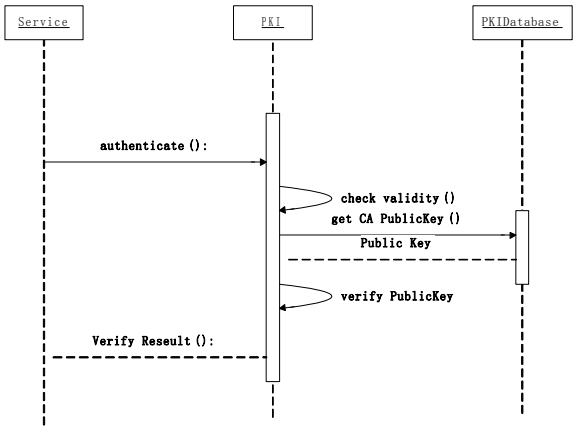

Fig. 5 Client request certificate authentication from PKI

5. RFID tags based anti-counterfeiting algorithm implementation

The above description strategies, this section use Hash algorithm, through the public network, realize tag and reader encryption decryption process.For any one tag, through the reader to read operation. Reader-side generated random number is set to R_{reader}, tag-side generated random number is set to R_{tag}.Each tag public network authentication server share a key $K_{tagserver}$, the key reader can not be detected. Each reader with public network authentication server share a key $K_{readrserver}$, and this key reader can not be detected.When the user use reader to read tag, $ReaderID, R_{reader}, K_{readerserver}$ exclusive or operation. After hash encryption M1, produced M_1 to the tag-side. Tag received M1, $ReaderID, R_{reader}, K_{readerserver}$ exclusive-or operation, Hash encryption, produced M_2.Reader received $M2$, the$M2, Rreader$ ， $Rtag$ with distributed server database;The server received data, Ergodic database database, detection $Rreader$ ， $Rtag$ existed. If presented, refused to request, if does not exist, will $Rreadr$ ， $Rtag$ into database, and return tag identifier, complete anti-counterfeiting process.

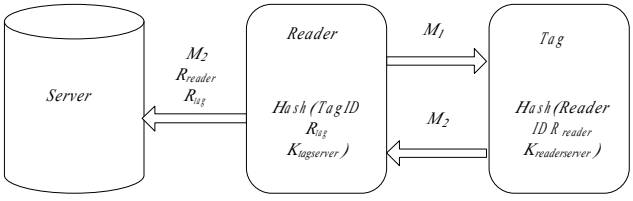

Fig. 6 RFID tags based anti-counterfeiting algorithm implementation

Protocol	Privacy	Replay Attack	DOS	Traffic Analysis	DB Synchronization	Performance
Hash-Lock	×	×	√	×	N	High
Randomized Hash-Lock	×	×	√	×	N	High
Hash Chain	√	×	√	√	N	High
Hash based ID variation	√	×	√	√	Y	Middle
Challenge-Response Based	√	√	√	√	N	High
David et al	√	×	×	×	N	High
LCAP protocol	√	√	√	√	Y	Middle
Karthikeyan-Nesterenko	√	×	×	×	N	Low
Duc et al	√	×	×	×	Y	Middle
Chien HY et al	√	√	1	√	Y	Middle
Masatakas et al	√	×	√	√	N	High
Cui Y et al	√	√	√	√	N	High

System code as follows :

Pseudo code

1) $R_{reader} \leftarrow Random(Reader);$

2) $R_{tag} \leftarrow Random(Tag);$

3) M:Message C:Cipheertext E:Enciphering D:Deciphering K:key;

4) $C=E_K(M);$

5) $M=D_K(C);$

6) $K_{tagserver}$ *(The Tag and Server shared key,Reader unknown)*

7) $K_{readrserver}$ *(The Reader and Server shared key,Tag unknown)*

8) $M_1=HASH(ReaderID \oplus R_{reader} \oplus K_{readerserver})$ *(Reader)*

9) $M_2=HASH(M_1 \oplus TagID \oplus R_{tag} \oplus K_{tagserver})$ *(Tag)*

10) Server←M_2, R_{reader}, R_{tag};

11) If (($R_{reader}R_{tag}$) *exist)*

12) Exit

13) Else

14) Put ($R_{reader}R_{tag}$,*Server)*

15) Return TagID

Table 1.Comparison between RFID tags and Transponders

6. dependability of the policy guarding against fakes

From the flow chat above, we can see, this security policy guarding against fakes includes tow processes in fact: Ⅰ, Security process contrasting digital certificates, namely, we compare digital abstract of digital certificate after verified and the paper digital abstract of digital certificate attached product to verify the certificate attached product truest or not; Ⅱ, Security process contrasting serial IDs, that is to say, throughout the method of comparing digital serial ID and serial ID printed on the RFID tag , we can verify whether the tow ID are accordant or not, and accordingly judge quality goods or fakes. The duple process of dealing with data and the application of encrpytion techniques insure this policy secure and credible.

7. Prospects

The technology of guarding against fakes has developed more than ten years. In the recent years, the market has been pressing for the technology of guarding against fakes more and more imminently along with the development of economy, and achieved more than 10 billions yuan [6]. But because of not exclusive, the prevalent paper stuff in guarding against fakes nowadays is easily copied just when one kind of new security technology is present soon. The technology guarding against fakes by products information retrospecting must become one kind of new research field of security. The future public information service system based on RFID must be one of important and handily flats guarding against fakes [7]. Security policy guarding against fakes based on RFID technology must bring us much more economic benefit and benefit society greatly.

References

[1] LANG Wei-min. RFID Technology and Application [M]. CHINA MACHINE PRESS, 2006, 6
[2] LI Yi-nong, PENG Lei, YUAN Hai, LI Fang-rong, LUO Huan-liang, HAN Biao. A RFID-based Digital Authentication System Against Counterfeit Export Wooden Package [J]. PLANT QUARANTINE, 2007, (5): 276-278
[3] JIAO Ya-bing. Building MIS of Internet of Things Based on RFID/EPC Technologies [J]. Packaging Engineering, 2010, (23): 116-119
[4] LI Ru-nian. Study on the Internet of Things Based on RFID Technique [J]. Journal of CAEIT 2009, (6): 595-597
[5] YU Hui-jun, ZHANG Xue-yi, WANG Xuan. Optimization of HF RFID System Performance [J]. Journal of Lanzhou Jiaotong University, 2008, (6): 114-116
[6] HU Xiang-dong, AN Dong-yang. Analysis and Design of RFID-based Logistics Tracking Management System in Automobile Manufacture [J]. Application Research of Computers, 2008, (12): 3829-3831
[7] WANG Jun-yu, LIU Dan, WEI Peng, MIN Hao. Research and Development of Anti-counterfeit System Based on RFID [J]. Computer Engineering, 2008, (8): 264-266
[8] The Electronic Product Code(EPC)- A Naming Scheme For Physical Objects", David L.Brock, http://www.autoidtabs.org/whitepapers/MIT-AUTOID-WH-002.pdf
[9] Sarma S E, Weis S A, Engels D W. RFID Systems and Security and Privacy Implications [C] //Proc. of the 4th International Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Germany: Springer-Verlag, 2003: 454－469.
[10] Masakazu Kanbe, Shuichiro Yamamoto.Ontology Alignment in RFID Privacy Protection.International Conference on Complex, Intelligent and Software Intensive Systems DOI10.1109/CISIS.2009,p718-723
[11] Rei Itsuki, Atsushi Fujita. Consideration for Efficient RFID Information Retrieval in Traceability System.IEEE Conference on Emerging Technologies & Factory Automation, 2009.
[12] Ming-Wen Chen,Jian Zhang,Song-Lin Hu.Covering-Based Routing Algorithms for Cyclic Content-Based P/S Overlays[J].Journal of Computer Science and Technology,2010,25(6):1214-1224.DOI:10.1007/s11390-010-1096-1.
[13] Ruisheng Shi,Fuqiang Liu,Yang Zhang等.An MID-Based Load Balancing Approach for Topic-Based Pub-Sub Overlay Construction[J].Journal of TSINGHUA UNIVERSITY ,2011,16(6):589-600.
[14] Wendong Zhao,Jin Zhang,Laixian Peng 等 .Assessment Algorithm for Service Matching Based on Bloom Filter[C].//2011 IEEE 3rd International Conference on Signal Processing Systems(ICSPS 2011).2011:128-132.
[15] Quan Z. Sheng,Sherali Zeadally,Aikaterini Mitrokotsa et al.RFID technology, systems, and applications[J].Journal of network and computer applications,2011,34(3):797-798.
[16] H.H. Cheung,S.H. Choi.Implementation issues in RFID-based anti-counterfeiting systems[J].Computers in Industry,2011,62(7):708-718.
[17] PANKAJ K. AGARWAL,JUNYI XIE,JUN YANG et al.Input-Sensitive Scalable Continuous Join Query Processing[J].ACM transactions on database systems,2009,34(3):13.1-13.41.
[18] Ryan H. Choi,Raymond K. Wong.Efficient Filtering of Branch Queries for High-Performance XML Data Services[J].Journal of Database Management,2009,20(2):58-83.
[19] Carlisle Adams, Steve Lloyd. Understanding PKI.Second Edition. Boston: Addison Wesley, 2002:28.
[20] United States General Accounting Office. Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology. Washington, D.C., 2001:74.
[21] United States General Accounting Office. Status of Federal Public Key Infrastructure Activities at Major Federal Departments and Agencies. Washington, D.C., 2003:7.
[22] Xingxin Gao, Zhe Xiang, Hao Wang. An approach to security and privacy of rfid system for supply chain.Proceedings of the IEEE International Conference on E-Commerce Technology for Dynamic E-Business (CEC-East'04), 2008.
[23] Wen Jun-Qin, "Design of a Multi-Source Information Collection and Retrieval System", JCIT: Journal of Convergence Information Technology, Vol. 7, No. 3, pp. 292 ~ 298, 2012
[24] M. Mahlouji and A. Noruzi, "Human Iris Segmentation for Iris Recognition in Unconstrained Environments", IJCSI International Journal of Computer Science Issues, Vol. 9, No 3, 2012.
[25] S. Nithyanandam, K. S. Gayathri, P. L. K. Priyadarsini, "A New IRIS Normalization Process For Recognition System With Cryptographic Techniques", IJCSI International Journal of Computer Science Issues, Vol. 8, No 4, 2011.
[26] Sungbum Park, Gyoo Gun Lim, Namgyu Kim,Sangwon Lee, "An ID-based Interoperation Method to Connect Digital and Physical Resources for Developing U-service: A Korea Mobile U-service Case using UCI and mCode", JCIT: Journal of Convergence Information Technology, Vol. 6, No. 7, pp. 382 ~ 396, 2011
[27] Jingxian Zhou, Yajian Zhou, Feng Xiao,Miao Zhang,Xinxin Niu, "Efficient and Secure RFID Mutual Authentication Protocol without Sharing Key", IJACT: International Journal of Advancements in Computing Technology, Vol. 4, No. 15, pp. 319 ~ 327, 2012

JIAO YABING: Shandong Yingcai University teacher, Master's degree in 2008, since 2012 in Dhurakij Pundit University PhD, the major professional direction information management.