A PKI-based Track and Trace Network for Cross-boundary Container Security

S.L. Ting[1], W.H. Ip[1], W.H.K. Lam[2] and E.W.T. Ngai[3]

**[1] Department of Industrial and Systems Engineering, The Hong Kong Polytechnic University
Hung Hum, Hong Kong, China**

**[2] Department of Civil and Structural Engineering, The Hong Kong Polytechnic University
Hung Hum, Hong Kong, China**

**[3] Department of Management and Marketing, The Hong Kong Polytechnic University
Hung Hum, Hong Kong, China**

Abstract

Challenges in container management, such as theft of products, cross-border smuggling, long checking time in processes of customs clearance and unable to track locations of products in real time, are currently faced by supply chain parties. In recent year, Electronic Seal (eSeal) technology is introduced to protect containers in a securely way. However, concerns related to data security increase when eSeal is applied in the track and trace infrastructure. To overcome this issue, this paper presents an idea to integrate the Public Key Infrastructure (PKI) in an eSeal device to enhance the cross-boundary container security.

Keywords: *Cross-boundary Container, Cryptography, Electronic Seal (eSeal), Public Key Infrastructure (PKI), Radio Frequency Identification (RFID), Track and Trace.*

1. Introduction

Logistics enterprises face tough competitions in an increasingly globalized market with new high and increased security requirements that response the efficiency of container movements in recent years. With millions of containers shipping around the world, containers are manually sealed so as to prevent cross-border smuggling, theft of products, and terrorist threats. With current practices, manual metal bolts, weld lock truck seals, cable seals and barcode seals are commonly used to prevent products to be stolen or broken when transporting from the point of origin to the destination point [1]. However, Zhang and Zhang [2] argued that these existing capabilities featuring in container security are vulnerable to guarantee the shipment integrity since there are numerous ways to defeat the manual seal, such as cutting holes in the side or top of a container and then repairing it. Thus, there is a pressing need to increase the security requirements of cross-boundary containers.

Attempted to address this issue, Radio Frequency Identification (RFID) technology is proposed to promote the container security [3, 4, 5]. RFID is an emerging technology that uses wireless radio to identify objects from a distance without requiring line of sight or physical contact. It can track the movements of objects through a network of radio enabled scanning devices over a distance of several meters [6, 7]. As stated by the academic study of Ngai et al. [8], RFID have been widely adopted in various industries like manufacturing, healthcare, logistics, and transportation. When it applies to the container security, an RFID-enabled seal, called an Electronic Seal (eSeal), is developed to allow importers, shipping companies, port officials and customs inspectors to determine, without a physical inspection, whether the seal has been tampered with and the security of the container compromised [1]. As stated by Kwok et al. [9], eSeal is a new way for improving issues of container management in global. For example, eSeal with RFID technology was rolled out at 20 lanes at Kaohsiung Harbor in Taiwan in 2009. Passive ultra-high frequency RFID tags embedded in eSeals, complied with ISO 17712, were used for identification of trucks in a port. Accuracy for read rate is higher than 95% with a truck travelling at a speed of 60 kilometers per hour and read range is more than 7 meters. The result showed that use of RFID-based seal in a port is able to reduce 6000 man-hours for escorts annually [10]. This implies RFID technology embedded in the eSeal is an effective approach to protect containers in a secure way.

RFID and eSeal technology has the potential to increase the container security; but this raises concerns regarding data security issues when implementing in a track and trace infrastructure (i.e. the container en route from the point of origin to the destination point) [11]. This is because all the product movement can be recorded by RFID technology among the entire supply chain in which such information (e.g. design of the distribution channel) may reveal private information regarding a particular business, like the business secrets about future strategic process

restructurings [12]. However, the academic literature addressing the security of the stored information in eSeal is scare. In particular, cryptographic measures in securing RFID data exchange in a track and trace infrastructure are almost absent. Yet, most studies were based on the electronic document which satisfies a pedigree requirement (i.e. ePedgree) [13, 14, 15]. Such approach can provide full supply chain visibility with detailed track and trace information in electronic format; but it cannot guarantee whether the container is moving on the right pedigree or not.

As a result of increased security requirements on RFID data protection in the track and trace infrastructure, cryptographic algorithms can be an important bridge between the efficiency of and security of data exchange process. Public Key Infrastructure (PKI) technology has such potential, in which it enables users to securely and privately exchange data through the use of a public and a private cryptographic key pair [16]. As discussed by Liping and Lei [17], PKI is a new security technology to establish trust relationship between parties in a secure network communications and online transactions. In addition to the applications domains like e-commerce and financial transaction environment, PKI is now applied in various areas. For example, Wilson [18] presented the use of public key certificates to secret the Unique Health Identifiers within an anonymous digital certificate. With the expected growth of m-commerce, Dankers et al. [19] tailored the PKI to enable end-to-end security for mobile systems. Considering the ensure the confidentiality and secrecy of the patient information, Brandner et al. [20] determined the user-oriented and legal requirements for a PKI for electronic signatures for medical documents.

With these successful applications mentioned in the literature, this paper presents an attempt to apply the asymmetric cryptography method (i.e. PKI technology) to strengthen the security in the data exchange of eSeal within the entire supply chain network (i.e. from their point of origin, while en route, through customs, and to their final destination). Apart from elaborating the use of the PKI in eSeal, this paper also introduces a PKI-based Track and Trace Network (PKI-TTN) to enhance the effectiveness of the cross-boundary container security.

The rest of this paper is organized as follows: Section 2 reviews the current track and trace infrastructure, eSeal technology and its security considerations in the data protection. The cryptographic method of the PKI-based Track and Trace Network (PKI-TTN) is presented in Section 3. Section 4 evaluates the performance of PKI-TTN and the conclusion is drawn in Section 5.

2. Track and Trace Infrastructure and eSeal Technology: Current Situation and Security Challenges

Track and trace infrastructure reflects the concept in tracking the current location of objects in the supply chain and tracing their past locations. In today's business world, the track and trace infrastructure of cross-boundary container has a tendency to get complex as the inspection tasks are done by multiple parties (e.g. shippers, forwarders, and consignees) [12]. Generally, there are three tasks to perform in each container terminals, namely container identification, seal checking, and damage checking. As reported by the study of Tsilingiris et al. [21], all these checking activities are inevitably repeated as the involved parties do not share the information to each other. As a result, checking time in processes of customs clearance is increased significantly.

Furthermore, another major problem encountered in the existing track and trace infrastructure is the theft of products and cross-border smuggling. Although manual seals are used to govern the control and management of containers, the influx of smuggling is constantly revoking [1]. As discussed by Bastia [22], the insufficient information transmission among supply chain parties makes them difficult in assuring the product lifecycle safety, especially the product authentication problems.

In order to fulfill the need for electronic infrastructure and information sharing platform, EPCglobal network was established for supply chain information sharing, especially for the flow of products in the supply chain [23]. Each product tagged with RFID label is assigned a universal unique ID called an Electronic Product Code (EPC) for the unique identification and tracking by different parties in the worldwide supply chain. It provides and promotes a standardized product identification mechanism and technology. To further satisfy the need for cost-effective and reliable hardware for cargo and container authentication and management, eSeal devices have been introduced during these last few years. Nowadays, there are a number of successful cases [2, 4, 9, 10], in many parts of the world showing that using RFID-based eSeal and information sharing platform can improve the efficiency and reduce cost of daily land logistic operations. For example, Kazakhstan and Lithuania customs authorities have been using RFID-based electronic seals on trucks passing through their countries since 2006. The system ensures that there is no unauthorized opening of cargo; and the location and status of the trucks transporting goods within their borders can be traced. It successfully helps to prevent smuggling and theft of cargo [24]. An increasing number of studies have been

conducted to evaluate the potential and benefits of the use of eSeal in container management.

So far, one problem arises when implementing eSeal technology in track and trace infrastructure is the data protection issues [12, 25]. Since much information related to the companies is contained in the RFID tag, therefore a secure solution in the data exchange process is essential to develop within the infrastructure. In particular, two security elements, namely confidentiality and integrity, are taken into consideration in the data protection issue. Confidentiality is concerned with the authentication for the access to data (i.e. only authorized persons or organizations can share the information); whereas the integrity is concerned with the completeness of the shared information (i.e. whether the information is being altered by others). Compared with the confidentiality, integrity is much more difficult to achieve as it requires to assess the trustworthiness of the source of the information [16]. Consequently, an increasing number of cryptographic methods have been developed for accomplishing these two security elements. Among these approaches, the PKI has been widely used because of its strong encrypted tunnel during the data exchange process as well as its well defined standard [26]. The distinguishing feature of a PKI is the use of a digital certificate issued by a trusted party, named Certification Authority (CA). The issued certificate is digitally signed using a CA's secret key to the messages specifying a user and the corresponding public key (Figure 1). Once the certification service is discontinued by a CA's key compromise, it will result in considerable degradation of the overall level of reliability and finally the fatal impact to the overall PKI [27].

Fig. 1 Digital certification

Regarding piracy and security are two issues to hurdle the RFID implementation [28], an increasing number of research activities [29, 30, 31, 32, 33] are focusing on employing PKI in the RFID systems, like the studies. Vaudenay [34] even pointed out that the use of public-key cryptography outperforms other security protocols. However, all these above mentioned research works are concerned with the identification protocols between the tag and the reader; in which the network (i.e. product flow) in the track and trace infrastructure is scare. Therefore, the present study focuses on the discussion of how PKI approach can be implemented as the authentication mechanism in the track and trace infrastructure.

3. PKI-based Track and Trace Network (PKI-TTN)

In order to fulfill the security requirements of eSeal and customs clearance applications, a PKI-based Track and Trace Network (PKI-TTN) including an eSeal device [9], eSeal middleware and public key infrastructure is developed. This network is developed base upon eSeal device that is designed and integrated with different logistics enabling technologies of RFID, Bluetooth, Wireless Network, Sensor and Global System for Mobile Communications (GSM). It is developed using standardization and modularization approaches, so that the eSeal device can be assembled by putting together different function modules to perform different features as well as adapt to different application requirements.

3.1 eSeal Device

An eSeal device is an integrated automatic identification device. It is developed in a modular-based structure (Figure 2). There are totally four modules, namely: Identification and Control Module, Communication Module, Sensor Module and Seal Module.

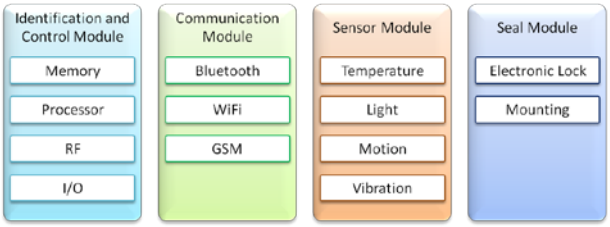

Fig. 2 Modular-based structure of an eSeal device [9]

Identification and Control Module: In Identification and Control Module, there is a processor and a memory for automatic identification purpose. This module also contains RF communication ability itself and serves basic identification purposes. It includes several input and output channels for providing additional features such as sound, light and Liquid Crystal Display (LCD). For additional functions, specific modules are designed (e.g. Communication, Sensor and Seal Modules). These can be plugged into the Identification and Control Module to extend the functionality.

Communication Module: The Communication Module is designed to extend the communication ability of the eSeal

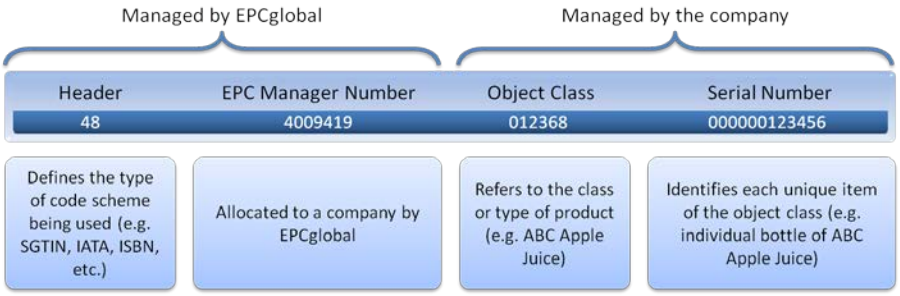

Fig. 3 EPC structure

device. By providing with different communication protocols, such as Bluetooth, GSM, and WiFi, eSeal device can communicate with different systems and devices.

Sensor Module: Senor Module is the plug and play modules of temperature sensors, light sensors, vibration sensors and motion sensors. It enables the eSeal device to monitor the environmental factors and record unexpected changes in the environment.

Seal Module: The Seal Module is a mechanical part and casting consisting of an Electronic Lock and Mounting. The Electronic Lock is designed as a changeable ID electronic lock. When the lock is opened, the ID of the lock will be changed. By tracking the ID change events in the log, the user can see whether the lock was opened authentically. In addition, the confidentiality and integrity of the information of this module is encrypted in a public key cryptography (see Section 3.3).

Standard Adoption of eSeal Device: In order to record the RFID information in a standardized and unique structure, RFID tag that features in EPCglobal specification is adopted in this study. It offers extended data capacity and employs a numbering scheme called EPC, which serves as a global standard to provide a unique ID for any item in the world [35]. With the license-plate type of identifier in EPC capability, real time tracking information on a product within its supply chain can be achieved [36]. Figure 3 depicts the structure of an EPC tag. Other than the four specific elements highlighted in the EPC structure, there is a reserve memory for advancing the security in data protection [37]. Thus, a PKI-based cryptographic approach is used to encrypt the tag information and the encrypted information is stored in such reserve space to protect the tag from malicious access.

3.2 eSeal Middleware

eSeal Middleware is developed to control and manage the functions and data exchange of eSeal device. It is a type of software which acts as a bridge between hardware devices and software systems, by providing connection, communication, configuration and management functions. With the aid of this, the data connected by the sensor module of eSeal device will be filtered, manipulated and transferred to the back end of the system. In general, eSeal Middleware consists of three components, namely adapters, filters, and loggers.

Adapters: Adapters are the components to connect various eSeal devices. In other words, they can control not only eSeal device mentioned in Section 3.1 but also the market available RFID devices.

Filters: Filters are the components used to filter and provide preliminary manipulation of the collected data from the hardware.

Loggers: Loggers are the output interface channels to connect to different backend systems. All the processed data will be sent to the desired destination via loggers. In order to support fast integration with applications already existing in the enterprises and organizations, the loggers provide standard data interchange protocols like Extensible Markup Language (XML), Hypertext Transfer Protocol (HTTP) and web service. Furthermore, the eSeal Middleware provides loggers to connect to public information sharing platforms (i.e. EPCglobal Network) to share the real-time supply chain information with logistics partners and related parties.

3.3 Public Key Infrastructure (PKI)

To enhance the data protection mechanism in the current data exchange process, PKI technology is employed to protect the real-time information captured in the RFID-enabled track and track infrastructure. Such a cryptography approach provides the advantage of delivering accurate supply chain information with immediate notification when there is any abnormality in the transportation process. Figure 4 shows the authentication mechanism for the container delivery from the point of origin to the point of destination. Before the shipment of the container, specific shipping information (e.g. shipper's information, receiver's

information, and delivery path) is identified and recorded in an XML format to form an electronic shipping document (Figure 5). In order to enhance data confidentiality (i.e. the information stored in the tag can only be read by the authorized party or user), a randomized one-off blind pubic key [38] is generated.

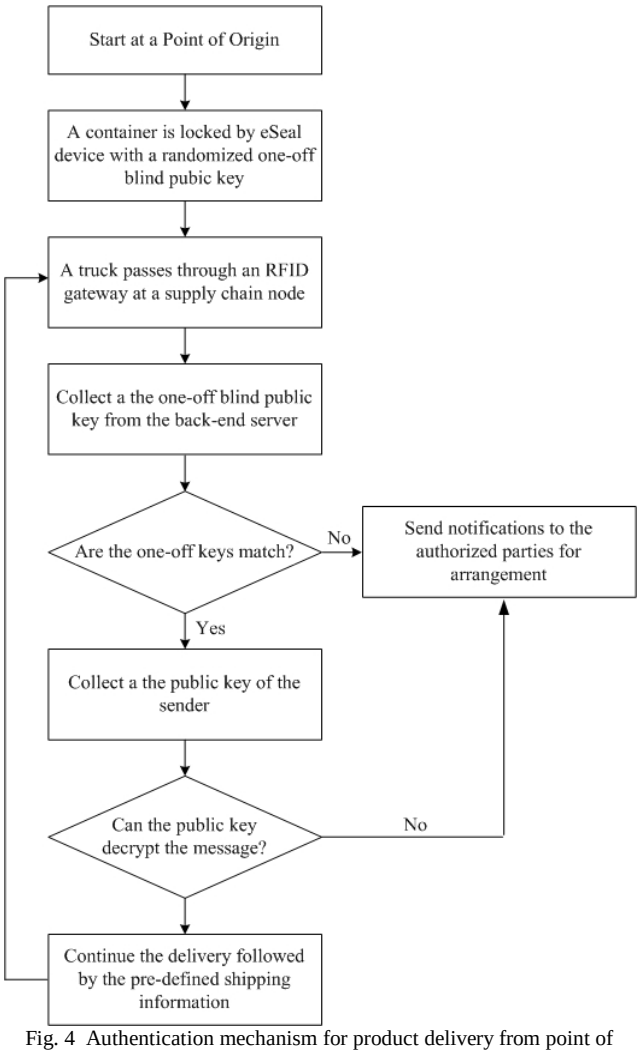

Fig. 4 Authentication mechanism for product delivery from point of origin to point of destination

Encryption Phase: Upon the completion of the setup of the electronic shipping document and the one-off key, an encryption based on the asymmetric key cryptography is employed to encode these two elements; and all these encrypted information are recorded into the reserve memory of RFID tag. Assume that there are four nodes (supply chain parties) in the track and trace infrastructure as described in Figure 5, the encryption procedures first start by encrypting the electronic shipping document by the private key of the manufacturer (i.e. $PrKey_{origin}$), the public key of the node C (i.e. $PuKey_C$) and the one-off key (i.e. $Key_{one\text{-}off}$) to form the first digital envelope (1st-DE). Then, the algorithm continues to encrypt the previous encrypted message (i.e. 1st-DE) by the private key of the manufacturer (i.e. $PrKey_{origin}$), the public key of the node B (i.e. $PuKey_C$) and one-off key (i.e. $Key_{one\text{-}off}$) to form the second digital envelope (2nd-DE). Next, the previous double encrypted message (i.e. 2nd-DE) is encrypted by private key of the manufacturer (i.e. $PrKey_{origin}$), the public key of the node A (i.e. $PuKey_A$) and the one-off key (i.e. $Key_{one\text{-}off}$) to form the third digital envelope (i.e. 3rd-DE). Finally, the triple encrypted message (i.e. 3rd-DE) is stored to the eSeal device. Such backward Nth digital envelope (Nth-DE) approach (i.e. "backward", in here, means that the algorithm encrypts the message from the end party to the first party and "N" is depending on the number of node in the delivery) can ensure the containers delivering in a right and efficient way. The encryption algorithm is depicted in Figure 6.

Decryption Phase: In contrast to the encryption phase, a decryption based on the asymmetric key cryptography is employed to decode the digital envelope. In this stage, each node is responsible to decrypt the corresponding envelope designed in the electronic shipping document. Take node A as an example, the algorithm starts by enquiring the one-off key (i.e. $Key_{one\text{-}off}$) from the back-end system and hence decrypting the 3rd-DE by the pubic key of the manufacturer (i.e. $PuKey_{origin}$), the private key of the node A (i.e. *PriKeyA*) and $Key_{one\text{-}off}$. If decryption is success (i.e. the keys are matched), the algorithm will update the encrypted message and the containers can keep going to next station. However, if a container goes a wrong way, there is a mismatch in the asymmetric key infrastructure. In other words, the digital envelope cannot be opened and alert message are prompted to the back-end system and immediate actions can then be taken. The decryption algorithm is depicted in Figure 7.

4. Performance Evaluation

A simulation is conducted to analyze the performance of PKI-TTN scheme in terms of key generation time, security and scalability. The simulation is operated on a Windows-based computer in Intel Core 2 Duo2.80 GHz with 2GB memory. The main objective of this simulation is to investigate the key generation time against the network size (i.e. the amount of network parties). The network size is set to 3, 6, 9, 12, and 15 in which the range can cover most of the real situation in today's supply chain network (i.e. the normal party involved in a track and trace infrastructure is 5 to 10). The average time taken to jointly generate the digital envelope is hence measured. Table 1 shows the time for key generations in terms of different network size. The generation time increases directly

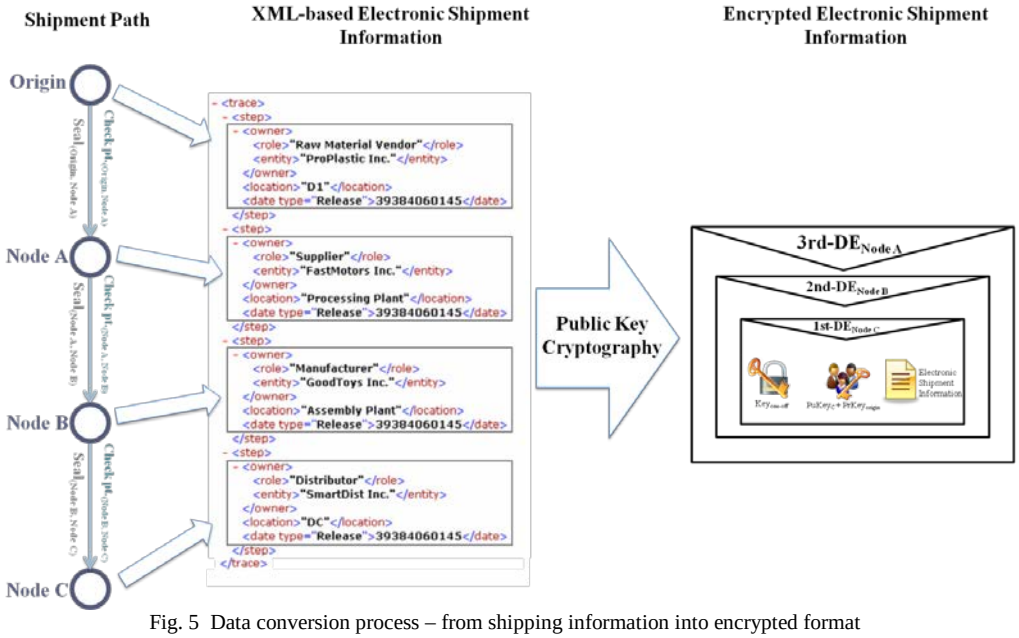

Fig. 5 Data conversion process – from shipping information into encrypted format

```
public Envelope pack(LinkedList<Site> siteList, Site shipper, Seal seal) throws Exception
        {
                Envelope existingEnvelope = null;
                /* from final destination to original source */
                for(int i = siteList.size() - 1; i >= 0; i--)
                {
                        Site site = siteList.get(i);
                        Envelope envelope = new Envelope();
                        envelope.setCheckPoint(site.getSiteId());
                        if(existingEnvelope != null)
                        {
                                envelope.setInterEnvelope(existingEnveloep);
                        }
                        envelope.encrypt(shipper.getPrivateKey(), site.getPublicKey(), seal.getOneOffKey());
                        existingEnvelope = envelope;
                }
                return existingEnvelope;
        }
```

Fig. 6 Pseudo code of encryption algorithm

```
public Envelope unpack(Envelope envelope, Site shipper, Site currentSite, Seal seal) throws Exception
        {
                envelope.decrypt(shipper.getPublicKey(), currentSite.getPrivateKey(), seal.getOneOffKey());

                if(envelope.getCheckPoint() == currentSite.getSiteId())
                {
                        /* if "envelope.getInterEnvelope()" returns "null" value, then it means the current site is
                           final destination */
                        return envelope.getInterEnvelope();
                }
                else
                {
                        throw new Exception("Invalid Check Point!");
                }
        }
```

Fig. 7 Pseudo code of decryption algorithm

proportional to the amount of network parties. The result is acceptable as it requires at most 30 seconds to generate the key set for the eSeal device.

Table 1: Key generation time against different network sizes

Network Size	Time (s)
3	0.39
6	3.88
9	11.28
12	15.73
15	32.55

In addition to the system performance, security analysis of PKI-TTN is also discussed in this section. As mentioned before, confidentiality and integrity are two important security elements to be ensured in the data protection of the current eSeal technology. In PKI-TTN scheme, the privacy of the electronic shipment information is protected by encrypting data streams as well as the messages via the asymmetric encryption. This action can prevent any unauthorized disclosure of information because only an intended recipient can get the corrected key set (i.e. the sender's public key and the eSeal one-off key) to decrypt the message. On the other hand, the integrity can be ensured by the PKI-TTN scheme in forms of the digital signature. With the property of cryptographic hash algorithm and signature algorithm, any change in the input message leads to any unpredictable change in the output message can be detected. In this case, if the data has changed, the signature is failure to verify, and hence the loss of integrity will be obvious to the recipient.

5. Conclusions

In recent years, critical issues, including theft of products, product counterfeit, cross border smuggling and invisible supply chain information, are penetrating in the current track and trace infrastructure. In cope with these challenges, RFID-tagged seals are proposed to securely protect high value of products delivered from a manufacturer to retailers. However, another problem related to the data protection raises in the RFID communication process. Thus, a framework for an integration of eSeal technology with public key cryptography is introduced in this paper. The information stored in RFID tags is securely protected by electronic envelope method with asymmetric encryption and decryption algorithms. Together with the electronic shipment information, a PKI-based Track and Trace Network (PKI-TTN) for cross-boundary container security is proposed to improve efficiency of product delivery, processing time at each supply chain node, and detection of cross-border smuggling in supply chain management.

Acknowledgments

The authors would also like to express their sincere thanks to the Research Committee of the Hong Kong Polytechnic University for providing the financial support for this research work (Project No.: 1-BB7Q).

References

[1] Organisation for Economic Co-operation and Development, Container Transport Security Across Modes, Paris: OECD, 2005.
[2] J. Zhang, and C. Zhang, "Smart Container Security: the E-seal with RFID Technology", Modern Applied Science, Vol. 1, No. 3, 2007, pp. 16-18.
[3] D. Mullen, "The Application of RFID Technology in a Port", Port Technology International, Vol. 22, 2004, pp. 181-182.
[4] F. Rizzo, M. Barboni, L. Faggion, G. Azzalin, and M. Sironi, "Improved Security for Commercial Container Transports Using an Innovative Active RFID System", Journal of Network and Computer Applications, Vol. 34, No. 3, 2011, pp. 846-852.
[5] E.W.T. Ngai, T.C.E. Cheng, S. Au, and K. Lai, "Mobile Commerce Integrated with RFID Technology in a Container Depot", Decision Support Systems, Vol. 43, No. 1, 2007, pp. 62-76.
[6] S.L. Ting, S.K. Kwok, A.H.C. Tsang, and G.T.S. Ho, "The Study on Using Passive RFID Tags for Indoor Positioning", International Journal of Engineering Business Management, Vol. 3, No. 1, 2011, pp. 9-15.
[7] J.P.T. Mo, and W. Lorchirachoonkul, "Design of RFID Cloud Services in a Low Bandwidth Network Environment", International Journal of Engineering Business Management, Vol. 3, No. 1, 2011, pp. 38-43.
[8] E.W.T. Ngai, K.K.L. Moon, F.J. Riggins, and C.Y. Yi, "RFID Research: An Academic Literature Review (1995–2005) and Future Research Directions", International Journal of Production Economics, Vol. 112, No. 2, 2008, pp. 510-520.
[9] S.K. Kwok, P.H. Ng, and K.L. Choy, "Development of an RFID-based Intelligent e-Seal System for Container and Physical Asset Management", Annual Journal of IIE(HK), Vol. 28, 2008, pp. 70-81.
[10] D. Friedlos, "Taiwan customs officials adopt RFID-enabled container seals", RFID Journal, 2001, Available at: http://www.rfidjournal.com/article/view/4727.
[11] B.L. Dos Santos, and L.S. Smith, "RFID in the Supply Chain: Panacea or Pandora's Box?", Communications of the ACM, Vol. 51, No. 10, 2008, pp. 127-131.
[12] L.W. Ferreira Chaves, and F. Kerschbaum, "Security and Privacy in Track and Trace Infrastructures", in D. Bouca, and A. Gafagnao (Eds.), Agent-Based Computing (pp. 109-122), New York: Nova Science Publishers, 2010.
[13] R. Celeste, and B.A. Cusack, "EPCglobal Standards in the Pharmaceutical Industry: Toward a Safe and Secure Supply Chain", Journal of Pharmacy Practice, Vol. 19, No. 4, 2006, pp. 244-249.
[14] S.K. Kwok, S.L. Ting, Albert H.C. Tsang, and C.F. Cheung, "A Counterfeit Network Analyzer Based on RFID

and EPC", Industrial Management & Data Systems, Vol. 110, No. 7, 2010, pp.1018-1037.

[15] L. Castro, and S. Fosso Wamba, "An Inside Look at RFID Technology", Journal of Technology Management & innovation, Vol. 2, No. 1, 2007,pp. 128-141.

[16] C. Adams, and S. Lloyd, Understanding PKI: Concepts, Standards, and Deployment Considerations, Boston: Addison-Wesley, 2003.

[17] H. Liping, and S. Lei, "Research on Trust Model of PKI", in Proceedings of the International Conference on Intelligent Computation Technology and Automation (ICICTA), 2011, Vol. 1, pp. 232-235.

[18] S. Wilson, "A Novel Application of PKI Smartcards to Anonymise Health Identifiers", in Proceedings of the AusCERT 2005 Asia Pacific Information Technology Security Conference, 2005.

[19] J. Dankers, T. Garefalakis, R. Schaffelhofer, and T. Wright, "Public Key Infrastructure in Mobile Systems", Electronics & Communication Engineering Journal, Vol. 14, No. 5, 2002, pp. 180-190.

[20] R. Brandner, M. van der Haak, M. Hartmann, R. Haux, and P. Schmücker, "Electronic Signature for Medical Documents - Integration and Evaluation of a Public Key Infrastructure in Hospitals", Methods of Information in Medicine, Vol. 41, No. 4, 2002, pp. 321-330.

[21] P.S. Tsilingiris, H.N. Psaraftis, and D.V. Lyridis, "RFID-enabled Innovative Solutions Promote Container Security", in Proceedings of the Annual International Symposium on Maritime Safety, Security and Environmental Protection, 2007.

[22] S. Bastia, "Next Generation Technologies to Combat Counterfeiting of Electronic Components," IEEE Transactions on Components and Packaging Technologies, Vol. 25, No. 1, 2002, pp. 175-176.

[23] F. Armenio, H. Barthel, L. Burstein, P. Dietrich, J. Duker, J. Garrett, B. Hogan, O. Ryaboy, S. Sarma, J. Schmidt, K.K. Suen, K. Traub, and J. Williams, "The EPCglobal Architecture Framework", EPCglobal Inc., 2007.

[24] C. Swedberg, "RFID Seals Provide Border Security in Eastern Europe", RFID Journal, 2008, Available at http://www.rfidjournal.com/article/articleprint/4032/-1/1.

[25] T. Yeh, Y. Wang, T. Kuo, and S. Wang, "Securing RFID Systems Conforming to EPC Class 1 Generation 2 Standard", Expert Systems with Applications, Vol. 37, No. 12, 2010, pp. 7678-7683.

[26] S.A. Brands, Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy, Cambridge, Mass.: MIT Press, 2000.

[27] B.M. Kim, K.Y. Choi, and D.H. Lee, "Disaster Coverable PKI Model Utilizing the Existing PKI Structure", in Proceedings of the Workshops On the Move to Meaningful Internet Systems, 2006.

[28] N.C. Wu, M.A. Nystrom, T.R. Lin, and H.C. Yu, "Challenges to Global RFID Adoption", Technovation, Vol. 26, No. 12, 2006, pp. 1317-1323.

[29] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede, "Public-Key Cryptography for RFID-Tags", in Proceedings of the Fifth IEEE International Conference on Pervasive Computing and Communications Workshops, 2007, pp.217-222.

[30] A. Wallstabe, and H. Pohl, "Implementing high-level Counterfeit Security using RFID and PKI", in Proceedings of the Third European Workshop on RFID Systems and Technologies, 2007, pp. 1-5.

[31] Y. Ham, N. Kim, C. Pyo, and J. Chung, "A Study on Establishment of Secure RFID Network Using DNS Security Extension", in Proceedings of the Asia-Pacific Conference on Communications, 2005, pp. 525-529.

[32] H. Deng, and W. Deng, "Identity Authentication in RFID Based Logistics-Customs Clearance Service Platform", in Proceedings of the Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2009, pp. 604-607.

[33] F. Armknecht, L. Chen, A. Sadeghi, and C. Wachsmann, "Anonymous Authentication for RFID Systems", in Proceedings of the Sixth Workshop of RFID Security, 2010.

[34] S. Vaudenay, "RFID Privacy Based on Public-Key Cryptography", in Proceedings of the Ninth International Conference of the Information Security and Cryptology, 2006.

[35] P. Lei, F. Claret-Tournier, C. Chatwin, and R. Young, A Secure Mobile Track and Trace System for Anti-counterfeiting, in Proceedings of the IEEE International Conference on e-Technology, e-Commerce and e-Service Hong Kong, 2005, pp. 686-689.

[36] EPCglobal, Inc., "RFID Implementation Cookbook", 2006, Available at: http://www.epcglobalinc.org/what/cookbook.

[37] K.H.M. Wong, P.C.L. Hui, and A.C.K. Chan, "Cryptography and Authentication on RFID Passive Tags for Apparel Products", Computers in Industry, Vol. 57, No. 4, 2006, pp. 342-349.

[38] J. Zhang, and X. Liu, "On the Security of ID-Based One-Off Blind Public Key", in Proceedings of the International Conference on Internet Technology and Applications, 2010, pp. 1-4.