UNATTENDED HOME DELIVERY SYSTEM BASED ON PKI TRUST MODEL IN URBAN AREAS

Bian Wenliang
School of Economic and Management, Beijing Jiaotong University, Beijing, China

Nie Xuyun
School of Computer Science and Engineering, University of Electronic Science and Technology of China Chengdu, China

Keywords: Physical distribution, Unattended reception, PKI.

Abstract: The unattended reception not only provides a convenient and alternative choice for family customers' reception, but also effectively improves the efficiency of physical distribution of enterprises. However, the system security of such a novel logistics model has hardly attracted people's attention. In this paper, we focus on the physical distribution for urban households' grocery, and construct a safe and trusted unattended home delivery system box based on Public Key Infrastructure (PKI) and its trust model. In order to promote its practical application in the process of modern logistics management, we also propose a series of recommendations.

1 PREFACE

Unattended reception model has been adopted in many countries where there's a developed logistics industry, such as America and Finland. It's also a good supplementary means for general attended reception model in home delivery. Moreover, in our fast-paced modern life in a big city, this model evidently has more convenience and efficiency compared with the attended reception one.

Nowadays, the increasing security risks spur consumers' growing awareness for safety of their lives and properties. As in the case of unattended states, customers can only passively accept the goods, the probability of safety problems to occur is significantly increasing. These risks may include delivered goods and receiving device being stolen, unknown materials being put in your device deliberately, and so on. Especially, in densely populated urban areas where people has some centralized delivery demands, post-office-box-like cargo receiving device can no longer meet people's need in receiving security. With the development of B2C e-commerce, the superiority of unattended reception model in the home delivery has drawn us an increasing attention. But how to design a safe home delivery system easily accepted both by customer and business? It's a problem in the context of urban home grocery purchasing. In this paper, we are trying to solve it.

2 LITERATURE REVIEW

With the B2C e-commerce development, such a situation has often taken place in which customer has no time to accept the delivery at home. Generally, the goods can be parked in the customer's neighborhood, and adjacent cargo collection points (such as a self pick-up point, collection of the post office, shops or kiosks, etc.) instead. Considering efficiency and safety, unattended receiving system has emerged (Hale, 2006). According to the difference in basic devices, this system can be divided into receiver box (Reception Box) model and delivery boxes (Delivery Box) model (Punakivi, Yrjölä and Holmström, 2001). A reception box is a customer-specific locked reception box installed in the customer's yard or garage, and it is usually refrigerated. Another type of reception box is a

Xuyun N. and Wenliang B.
UNATTENDED HOME DELIVERY SYSTEM BASED ON PKI TRUST MODEL IN URBAN AREAS.
DOI: 10.5220/0003268000030008
In *Proceedings of the Twelfth International Conference on Informatics and Semiotics in Organisations (ICISO 2010)*, page
ISBN: 978-989-8425-26-3

reception locker, which consists of several reception boxes and can be installed, for example, in car parks or railway stations.

To address the above unattended receiving issue, many efforts have been made. Although a certain amount of initial investment, Punakivi et al. have demonstrated that when a company faced a stable demand or a development of a large number of customers who purchased goods repeatedly the unattended reception model based on the reception box is very appropriate (Punakivi, Yrjölä and Holmström, 2001). Home deliveries with customer specific reception boxes allow 44 to 53 % cost savings and shared reception boxes even 55 to 66% cost savings compared to the attended reception with 2 hours delivery window (Punakivi, 2003). Delivery box is an insulated secured box equipped with a docking mechanism. Goods, together with the delivery box were left at the dock location and fixed, and then the empty containers that customers dump for goods will be collected in the course of the next delivery, or after some time. Each customer requires only a little investment, which will make it possible for company to expand rapidly and operate flexibly. However, the disadvantage is that the collection of empty containers will bring an additional cost and affect the entire family delivery system efficiency. Kallio (Kallio, Kemppainen, Tarkkala and Tinnilä, 2000), Kämäräinen (Kämäräinen, Saranen and Holmström, 2001), Punakivi (Punakivi and Saranen, 2001) et al., with some applications such as simulation and mathematical model, compare with a variety of family delivery program to study the efficiency and impact toward unattended reception in the home delivery process. In addition, the existing studies mostly concentrate in the Nordic areas with a sparsely population, such as Finland. Punakivi et al. recommend that a further research on unattended reception pattern in densely populated urban areas is needed (Punakivi, Yrjölä and Holmström, 2001).

The existing researches on the unattended reception model lead to maintain a high operational efficiency without sacrificing service levels. These have provided a guarantee for the development of the grocery retail industry, especially for the associated online retail industry. However, these distribution patterns have their limitations. For instance, with the receive box model it requires additional investment on the customers end. So it doesn't meet the demand of physical distribution for the suburban customers. The delivery box model need to recycle empty containers frequently to reduce the delivery efficiency. This doesn't satisfy the concentrated requirements of physical distribution in urban center. How can we take the advantages of both models into full account in the practical application is worth studying. Moreover, according to the analysis of our all knowledge and retrieved literature, existing studies on this issue with family security consideration are rarely addressed. An analysis of system safety is also hardly found in most researches, except that McKinnon et al. explored general security issues on the unattended reception model (McKinnon and Tallam, 2003). However, we know that more and more people are concerned about the safety of their lives and property, so the relative research must be put on the agenda in logistics areas.

Publics Key Infrastructure (such as X.509-based schemes (Kent, 1993)) has been used in so many fields. Essentially, it's a useful tool to indicate and manage the relationship of trust. Moreover, this trust model can also be embedded in the framework of some applications, such as P2P (Peer to Peer) sharing and e-commerce (Fang, 2007; Kambourakis, Rouskas and Gritzalis, 2004).

3 SYSTEM DESIGN

3.1 Idea for System Construction

We take into account all enterprise physical distribution efficiency, customer demand and system security, and then establish a unified unattended home delivery system in urban areas. In fact, the benefit of reception-box-based system applied in a concentrated demand area will arrived at a scale economies effect with an increasing of requirement, while the facilities of a delivery-box-based system applied in a scattered demand area will be able to share among different customer's families. Therefore, in the course of application, two kinds of physical distribution patterns should be coordinated and combined based on the characteristics of urban areas in our country. Specifically, according to the differences of urban households living conditions we propose an unattended home delivery system with a necessary security thinking, which consists of three types of unattended delivery models.

i. In response to the communities with concentrated requirement and high-density living condition, we design a community-specific reception box model for them;
ii. For urban households in lower-density living condition, we design a home reception box

model for them;

iii. And for households in peri-urban areas, we design a delivery box model for them.

These three types of models should make adequate adjustment in order to assort with the economic development and living condition of different cities. In respect to security of the system, the PKI technology is used to guarantee the securities of accessing, communicating and authorizing with mutual trust.

3.2 System Composition

In this paper, the unattended home delivery system based on PKI trust model consists of the Trusted Center, reception facilities, communication equipment, household customers and shipping companies.

The Trusted Center is an authoritative third-party digital certification management center operated by a neutral institution, or government department, also it is the core of PKI system. The Trusted Center can ensure that a specific digital certification is the authorized person. In the application of data security and e-commerce it is used to confirm the true identity of each participant when the information is changed. Essentially, the Trusted Center is a Certification Authority (CA), which is responsible for issuing certificates, authenticating certificates, and managing a provided certificate.

There are three kinds of reception facilities. A reception box is a customer-specific locked reception box installed in the customer's yard or garage. Another type of reception facility is a reception locker, which consists of several reception boxes and can be installed, for example, in car parks or railway stations. The third option is a delivery box, which is an insulated secured box equipped with a docking mechanism. These reception facilities are free or lower cost for customers. Moreover, some facilities must have a certain computing and storage capacities (such as the hash function computing, digital certificate storage), and be able to maintain a stable communication with the Trusted Center.

Communications equipment is accessorial part of the system which is used to keep the date transfer in security. It includes communication terminals for customers' command input and information reception, business users (by computer, PDA or cell phone), and the network connection facilities.

Household customers and shipping companies are the system users. A shipping company may be a manufacturer, retailer or logistics company. Among them, shipping companies consist of some trusted delivery companies with credible certification and some casual delivery companies without credible certification.

3.3 System Process

We here demonstrate the operational process of the unattended home delivery system. To simplify and clarify, we separate it into five kinds of operations and depict them respectively in Figure1-3.

(1) Establishment of a trusted relationship: The company and customer set a long-term opening service letter after a consultation between the enterprise and customer. Then one authorized by the Trusted Center should digitally sign the letter to initiate an opening application. The Trusted Center authenticates the application with the public key for the authorized customer or company. When the authentication is passed, the Trusted Center will provide digital certificates and a key-tool (such as USB-Key, or radiofrequency card) for the applicant, where the digital certificate stores a public key, as well as the key-tool stores a private key. In order to realize a short-term delivery for some household customer, company and customer set a one-time service letter with a time stamp after an oral agreement. Then one authorized by the Trusted Center should digitally sign the letter to initiate a temporary application. The Trusted Center authenticates the application with the public key for the authorized customer or company. When the authentication is passed, the Trusted Center will provide authorized one a time-limited password, and write the hash values of password and time stamp into the reception facilities memory.

(2) Delivery process under reception box model: In the course of delivery by authorized company, the delivery person first enters the user name and password (manually or automatically), then the terminal of reception box checks the password with hash function by comparing the value listed in the terminal memory. If it is correct, the delivery person will be prompted to insert the key-tool. When the key-tool is inserted, the terminal of reception box reads user's private key. Then the system generates a random number, and signs this random number with the private key. Next, the system uses the public key in digital certificate of the trusted company stored in terminal to authenticate the signature. If the authentication is passed, the door opens and delivery is available. However, the delivery of a general company (non-trusted) is relatively simple. First, the delivery person inputs the user name and password

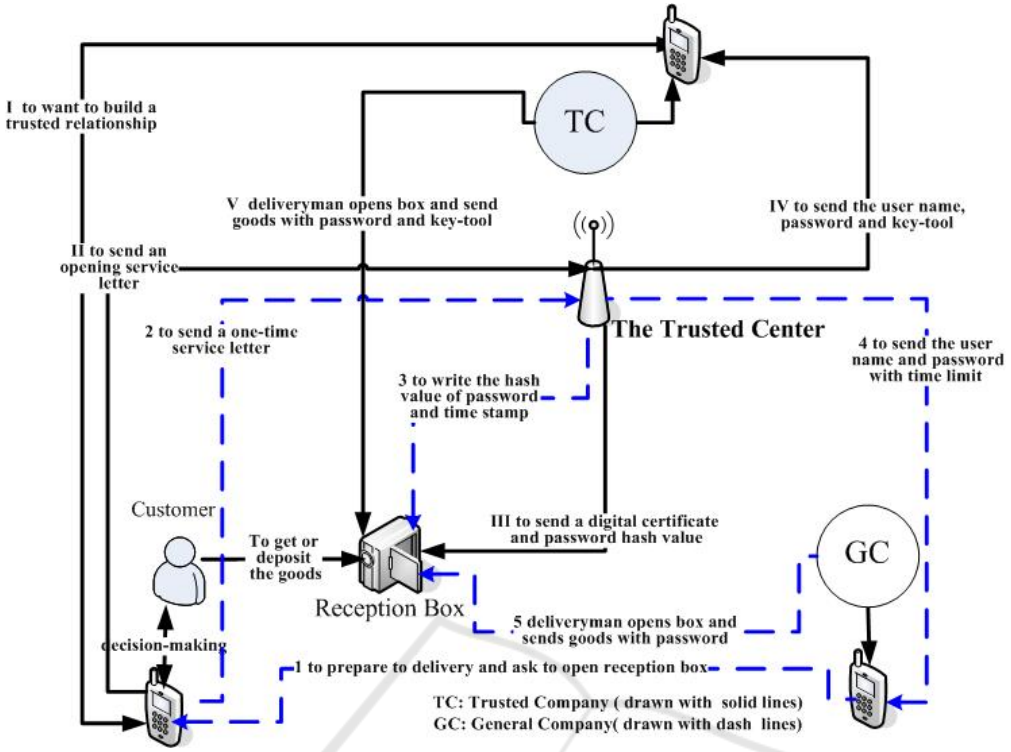

Figure 1: The process of the reception box model in detail.

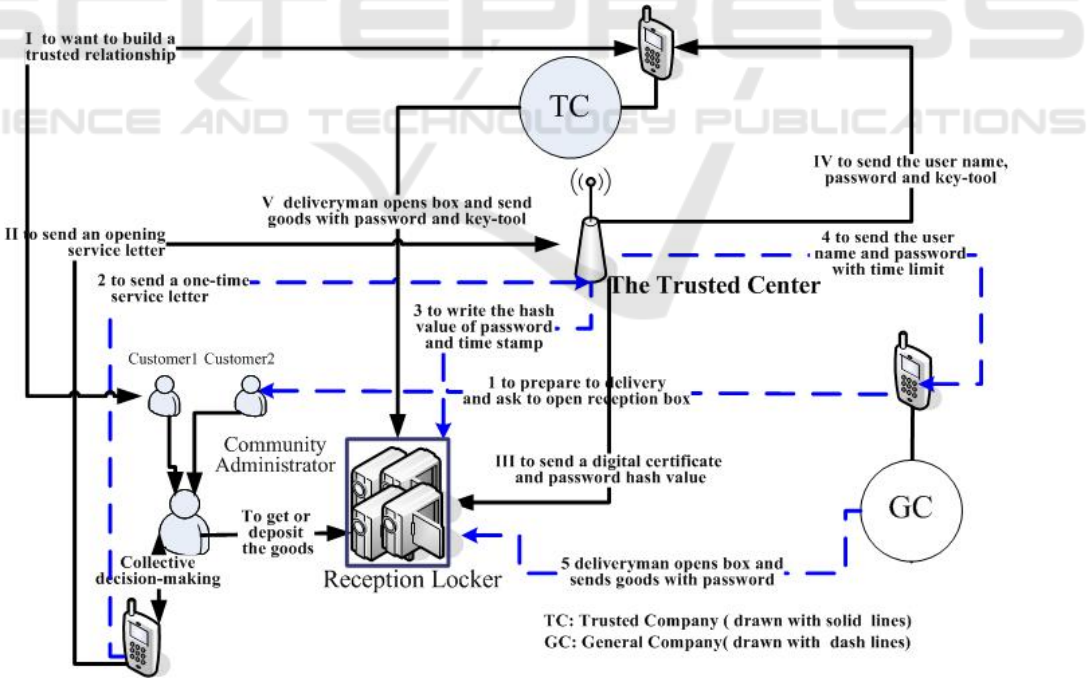

Figure 2: The process of the reception locker model in detail.

obtained temporarily, the terminal of reception box checks the password with hash function whose result is compared with the value listed in the terminal memory. If the value is just in the list and system time does not exceed the time limit, the door opens and delivery is available.

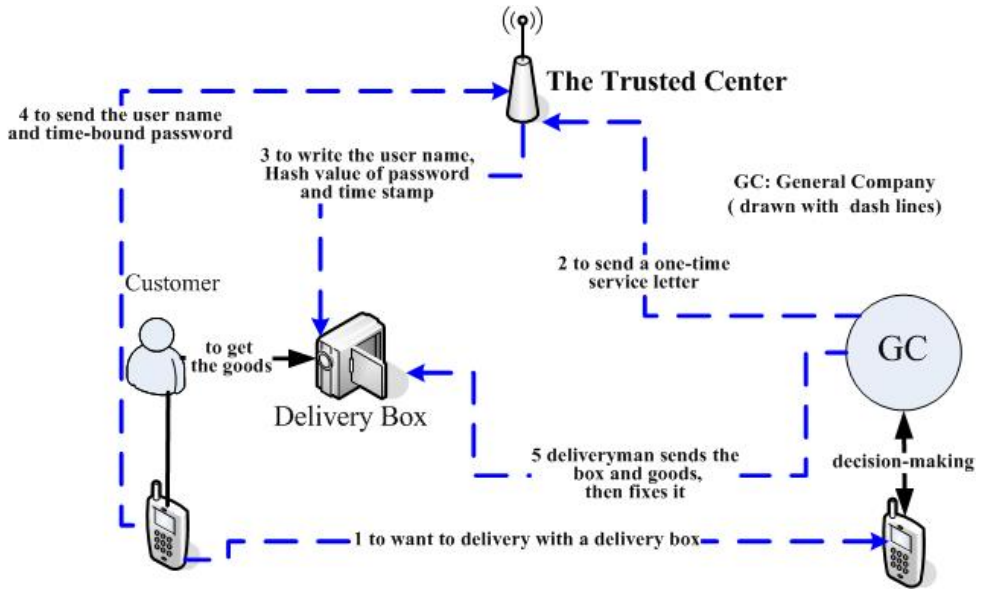

Figure 3: The process of the delivery box model in detail.

(3) The delivery process under delivery box model: Through the Trusted Center the authorized company sends a user name and time-bound password to the customer who needs a delivery. Then it writes the users' names and hash values of their password into the terminal of delivery box. Finally, the goods together with delivery box and it's sent to customer's home in a specify location.

(4) Pick up process: This process should be finished by the customers. Near their house, the terminal system of reception facilities stores a list of user names and password hash values issued by the Trusted Center, even the user's digital certificate. Under the delivery box model, as the household user first enters a user name and password, the terminal computes a hash operation of the password, and compares its hash value with the corresponding values in the stored list. If the comparison is OK and the prescribed time constraint is satisfied, user can open the box. Under the reception box model, except the above operations, users need to insert a key-tool. Then the terminal reads the user's private key and as sign a new generated random number. And it provides an authenticate signature. When passed, the door opens and the reception is available.

(5) Pick up management in a community: There is no essential difference between a community user and a general customer in respect of application and delivery. But as far as the pick up process is concerned, the community user slightly differs from the latter. First, we need to arrange a person as a reception locker manager, a unified "customer" facing a number of delivery companies. The users in a community apply to open reception locker with their own user password and the community manager controls a common key for whole customers. This community manager can be a part-time job, and he or she also can apply for opening the locker authorized by the Trusted Center in order to deal with the expired unclaimed goods.

A two-factor trust authentication is adopted in this system process, which supports a local safety feedback and a remote trust transfer among the Trusted Center and all kinds of users. Though some additional tasks are added to users, this system helps us to avoid the intervention by unknown companies and the passive reception from unknown items. Additionally, it takes into account the confidentiality of information communication and customer family's security.

4 ABOUT IMPLEMENTATION

The establishment of unattended home delivery system is a systems engineering, so the implementation of relevant technique and management will directly affect the success of whole system. Here, three following proposals are put forward by us in system implementation phase to improve the entire efficiency.

Proposal for construction and operation: First of all, we should confirm the main body for construction and management. There must be an authoritative and neutral third party responsible for

the facilities pre-investment and network construction for entire system, which should be in charge of the centralized management of a trusted certification. It is pivotal to ensure social benefits of the system. Second, in the operational process, the integration within the building of this system, our society credit system and online payment system is needed, which ensures a good exogenous environment for implementation.

Recommendation for business development: Because the system requires that the customer must have a basic on-line operational capability, we recommend that the system operation can integrate with the construction of intelligent community, intelligent building, and so on. As a first step, to establish a benchmark, a demonstration base can be set in high-end communities initially. Gradually, it can extend to other similar areas. At the same time, the system needs not only good information sharing between the various delivery models under the coordination of the Trusted Center, but also a seamless information interface linked with the traditional on-site reception model.

Proposal for business extension: Many additional and value-added business can be explored using the advantages of resources and security of this system. For example, customers can also safely transfer their own goods through the located household reception boxes. In detail, a reception box can contain some temporary inventory which will be expected to send to other people. Just following a simple trusted authority it can be taken by the other one in the case of unattended situation. Additionally, the reception boxes concentrated in a region can be centralized and managed by a similar community-based means with more secure and intelligent.

5 CONCLUSIONS AND FUTURE RESEARCH

In this paper, we propose an unattended home delivery system to meet the physical distribution needs of different urban regions and their requirement of home security. As well as a useful complement to the traditional on-site delivery system. In this system, a variety of delivery equipment is the carrier for system operation and the mature PKI technology is the basis. This study focuses on the basic ideas proposal of the system construction and the technical feasibility, the economic feasibility analysis and detailed methods for the implementation still need some further study.

We also did not mention the alternatives to passwords (such as biometric methods of authentication), that provide a better form of underpinning paradigm for our solution in future.

ACKNOWLEDGEMENTS

We are especially grateful to the National Soft Science Research Program (Grant No. 2008GXQ6B135). Finally, we wish to thank two anonymous reviewers whose careful reading and thoughtful comments led to many improvements in the paper.

REFERENCES

Hale J. J., 2006. Secure unattended delivery system. *US Patent (NO. 10/347,742)*. App. 11/530,368

Punakivi M, Yrjölä H, Holmström J, 2001. Solving the last mile issue: reception box or delivery box? *International Journal of Physical Distribution & Logistics Management*, 31(6): 427 – 439.

Punakivi M., 2003. Comparing Alternative Home Delivery Models for E-Grocery Business, *Doctoral Dissertation*, Department of Industrial Engineering and Management, Helsinki University of Technology, Finland.

Kallio J., Kemppainen K., Tarkkala M., Tinnilä M., 2000. New distribution models for electronic grocery stores, *LTT-Research Oy Publications,* Helsinki.

Kämäräinen V, Saranen J, Holmström J, 2001. The reception box impact on home delivery efficiency in the e-grocery business. *International Journal of Retail & Distribution Management*, 31(6): 414 – 426.

Punakivi, M., Saranen, J. 2001. Identifying the success factors in e-grocery home delivery. *International Journal of Retail & Distribution Management*, 29 (4):156-163.

McKinnon A.C., Tallam D. 2003. Unattended delivery to the home: an assessment of the security implications. *International Journal of Retail & Distribution Management*, 31(1): 30-41.

Kent S. T. 1993. Internet privacy enhanced mail. *Communications of the ACM*, 36(8):48-60.

Fang D. 2007. Security Framework of E-Commerce Based on PKI. *Ship Electronic Engineering, 04*

Kambourakis G., Rouskas A., Gritzalis S., 2004. Performance evaluation of public key-based authentication in future mobile communication systems, *EURASIP Journal on Wireless Communications and Networking*. 1:184-197.