Research of Security Authentication for Railway Passenger and Freight e-Commerce

Xue Hu, Yang Li, Lei Meng, Jisheng Li, Xianning Tian, and Yong Zhang

***Abstract*—Based on the E-commerce standard system of China, this article includes an in-depth study of the railway passenger and freight E-commerce security technologies, describes the related contents of E-commerce security certificate for railway passenger and freight, builds security system architecture of the E-commerce ticketing system, and introduces the personal identity digital certificate authentication process and its basic requirements of the railway passenger and freight E-commerce. And finally, the importance of security certificate for railway passenger and freight E-commerce informatization is given.**

***Index Terms*—Railway passenger and freight, e-commerce, security authentication**

I. Introduction

With the development of market economy, the competitors increase their strength, the advantages of railway are weakened, and the railway is facing increasingly fierce competition. The railway only take full advantage of the new technologies, new means to transform the traditional operating model, can it win the competition in the market again. The growth of E-commerce brings new opportunities for the integration of information resource, the improvement of railway transportation service level, and the progress of harmonic railway construction. [1] And also, it provides a great inspiration for the railway to build a new E-commerce information platform.

In order to improve the information platform, we must guarantee the safety, stability and reliability of the railway E-commerce. The platform should have the abilities to bear the load brought by peak access volume, resist the risk from the Internet, and also guarantee the security, integrity of the information, the non-repudiation of information exchange. [2]

The security certificate of railway passenger and freight E-commerce is an information certificate service for trading partners in the railway passenger and freight operation, which is with the E-commerce technology as the core and combines the characteristics of railway passenger and freight transport. The E-commerce certificate technology is an encryption technique which takes the Electronic Certification, also known as Digital Certificate, as the core. It encrypts and decrypts the information transmitted in the internet, adds and verifies the digital signature based on the PKI technique. Security certificate is the core link of railway passenger and freight E-commerce; it insures the security, integrity and non-repudiation of information transmitted in the internet, guarantees the safety of network application, and makes the operation of railway passenger and freight E-commerce successfully and continuously.[3]

Manuscript received November 15, 2012; revised March 29, 2013.

Xue Hu, Yang Li, Lei Meng, Jisheng Li, and Yong Zhang are with the Center for High-speed Railway Technology, Tsinghua University (e-mail: huxue0214@163.com, nancylee1989@126.com, zhangyong05@tsinghua.edu.cn).

Xianning Tian is with the Easyway Company Limited.

II. The Security Issues for Railway Passenger and Freight e-Commerce

A. Security of Service Platform

The security of service platform includes system security and network security. System security such as application error, hardware failure, system software error and computer viruses can harm the effectiveness and reliability of the e-commerce system. For the security of the network, malicious attacks and destruction of the system are needed to be prevented.

B. Security of Transaction

Transaction process should protect the information flow of passenger and freight safe and reliable, and is not easy to be robbed and tampered, which requires to ensure the security of transactions, transaction information authenticity, authentication and non-repudiation of identity, and to protect the trade secrets not to be stolen.

C. Security of Internal System

The railway TMIS is connected with Internet, freight information flows in TMIS all the time, it is the basis of protection of the Railway Logistics normal operation, internal systems must be guaranteed not to be subjected to security threats from the Internet, which ensure the integrity, authenticity and correctness of data.

D. Security of Online Payment

The fund flow of the railway passenger and freight on the Internet flows inevitably. Therefore, to ensure online payments and the cost of clearing safe and reliable is one of the focus factors of the system implementation.

III. The Security Countermeasures for Railway Passenger and Freight e-Commerce

A. The Security Countermeasures for Service Platform

1) To implement physical security of computer network equipment and facilities, to avoid exposure to natural disasters;
2) The system security refers to the security of the host and

DOI: 10.7763/IJCTE.2013.V5.807

server, it is primarily to prevent application error, hardware failure, system software error and computer viruses, when the problems mentioned above occurs, an experienced administrator should fix the breakdown in time and restore the normal operation of the system;

3) To protect the operation security of the network, with contingency measures for emergencies, such as real-time data backup and recovery;

4) The safety of LAN or subnet is the outstanding problem of the current network security. Therefore, it needs to establish a system access control, intrusion detection and audit analysis mechanism to prevent the illegal invasion of internal or external personnel. Set up a firewall is essential measures to protect the security of E-commerce system network of railway passenger and freight.

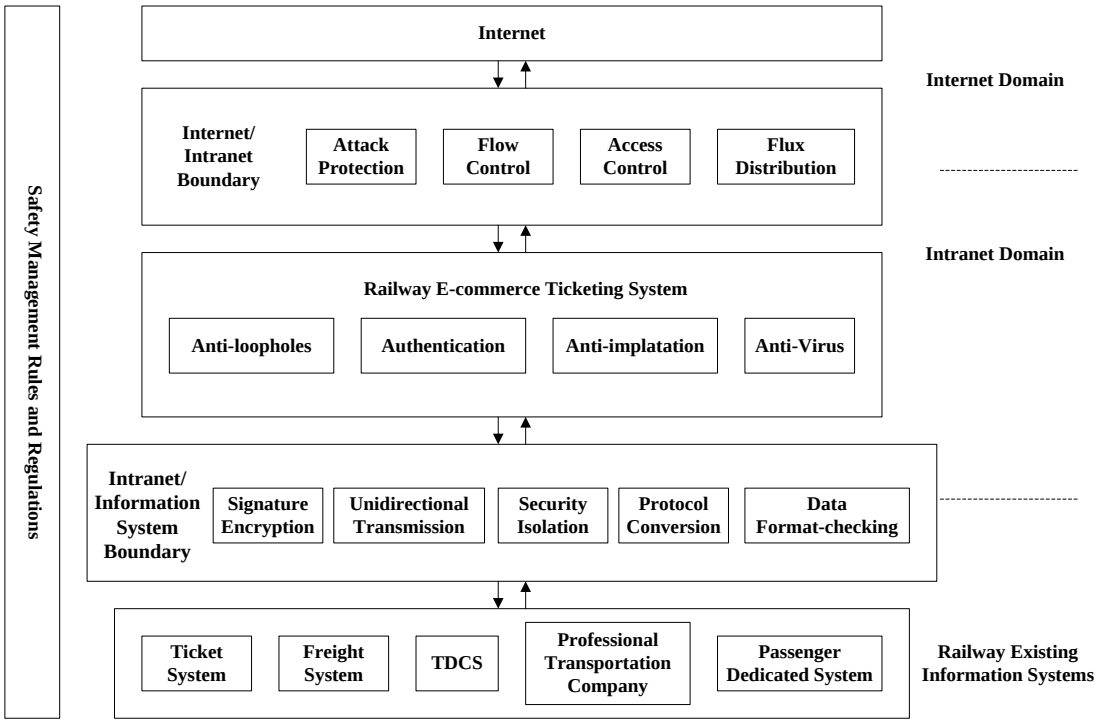

Fig. 1. Security system architecture of the e-commerce ticketing system.

A. The Security Countermeasures for Transaction

The authentication service is to identify the identity of the trading parties, to provide a guarantee for the authenticity of the identity. Access Control Service is to control the use of resources by authorization, to prevent unauthorized use or control of resources, which facilitate trade information confidentiality, integrity and controllability. Confidential services provide confidentiality guarantees for e-commerce participants in the storage, processing and transmission, to prevent the information from being leaked to unauthorized users. The undeniable Service is aim at threats from legitimate users, to provide undeniable evidence to resolve the dispute for denying support for the parties to the transaction.

Most of the E-commerce transactions of railway passenger and freight are larger transactions. Therefore, while ensure the security of the transactions technically, there is a need to limit trading service object to some extent, such as membership system, evaluation trader credit, etc.

B. The Security Countermeasures for Internal Systems and Online Payment

Internal systems and online payment security is mainly involved in information security technologies. In order to protect the security of data transmission, data transmission encryption technology and data integrity authentication technique need to be used.

To achieve the railway passenger and freight E-commerce system, connected with TMIS is inevitable. To guarantee TMIS security, firewalls between the E-commerce application platform and internal TMIS network needs to be established, and data encryption technology need to be used to transmit and store sensitive information.

E-commerce online payment and settlement of costs, from a technical point of view, the electronic purse, and payment gateway and safety certification are involved. Choose a third party certification to solve the security problems of the flow of funds is effective. The railway passenger and freight E-commerce should choose the China Financial Certification Authority as a fair and trustworthy third party certification. All parties involved in the railway passenger and freight E-commerce transactions must obtain the authentication of the China Financial Certification Authority and its affiliated certification, which means that all users have passed audit by the RA audit authorization department, and obtain a digital certificate issued by the issuing department.[4] In the transaction process, clients take advantage of the certificate matched comparison among the buyers, merchants and payment gateway, to verify the legitimacy of the transaction, and establish a trust relationship to complete the transaction.

Generally speaking, the railway passenger and freight E-commerce trading activity is carried out in the Internet, in view of the confidentiality and integrity of the transaction data,

the trading data transmitted on the Internet must meet the SSL protocol and the SET protocol, which is to ensure the transaction data are flowing in a secure channel, and to protect the efficiency of the transaction.

IV. The Security Architecture of Ticketing System Architecture for Railway Passenger and Freight E-Commerce

Based on the existing security system, the railway E-commerce ticketing system is built, which ensures important security boundary safe and enhance protection progressively. [4] Fig. 1 shows the security system architecture of the E-commerce ticketing system.

According to the application deployment architecture of the railway E-commerce ticketing system, this system is divided into three security domains and two security boundaries. [5] The security domains are internet, intranet and the railway information system. And the boundaries are internet/intranet boundary and intranet/information system boundary. The first boundary ensures across-domain accessing securely by using several security means. On the other hand, the protection of second boundary needs to be designed based on the security level of core network, and achieves bidirectional data exchange through security isolation and information exchange system.

The railway e-payment platform is not only connected with related railway internal business systems and doing business processes, but also exchanges information with railway external systems such as certification center, banks, and third-party payment. The railway existing system requires a higher level of security, but the construction of the e-payment platform system should not reduce the security level of the original system. Two systems, the extranet system which contacts with railway external system and the intranet system which contacts with railway internal business system, should be built using safety protection means to ensure intranet securely.

V. Personal Authentication of Railway Passenger and Freight E-Commerce

The booking system handles service request and gives feedback through the online E-commerce management, like searching, booking, ticketing, etc. In order to ensure the booking system to obtain real-time data of the ticket, and achieve the booking services online or by phone successfully, and also to guarantee that the ticket data of ticket system is relatively independent and the ticket server security, railway passenger and freight e-commerce personal authentication must be standardized to ensure the confidentiality of the data, the integrity of the information, and the identity of the authentication and non-repudiation.

A. Personal Authentication System of Railway Passenger and Freight e-Commerce

It is said that PKI is the core of the information security technology, and also is the key and foundation of e-commerce technology. The complete PKI system must have the following basic components: certificate authority (CA), digital certificate repository, the backup and recovery system of key, certificate revocation system, and application programming interface (API). [6]

1) Public key infrastructure

The Public Key Infrastructure technology is currently used in order to solve the problem of Internet security. PKI technology uses certificate to manage public key, bounds the user's public-key and other identifying information such as name, E-mail, and ID of the user, and verifies the user's identity on the internet through third-party trusted institutions.

At present, in order to ensure the secure transmission of information, the general approach is using digital certificates built on the basis of PKI to encrypt and sign the digital information to be transferred to ensure the confidentiality of the information transmitted.

2) PKI structure

The PKI structure is shown as below, and some concepts are defined as follow.

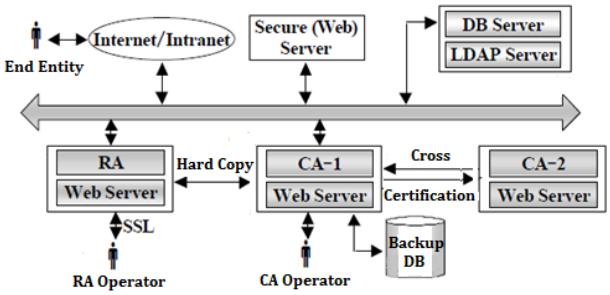

Fig. 2. PKI structure.

CA Server is the core of the whole CA. Its major functions include developing certificate policy, RA initialization, accepting request of RA signed, revoked and update the certificate, generating a key pair for end entity or subordinate CA, signing, revoking, and updating the certificate, publishing certificates and the certificate revocation list, signing cross-certificate, as well as key escrow and recovery.

The major features of Registration Authority, or RA for short, include accepting end entity requests to identifying the user's identity, submitting requests to the CA to sign, revoke and update certificate, releasing the certificate and CRL issued by the CA, and notifying the user to obtain a certificate.

LDAP Server provides services to browse the catalog, and is responsible for adding the user's information and digital certificate to the server. So that users will be able to get digital certificate of other users by accessing the LDAP server.

Database Server is the core part of CA. It is used for the storage and management of data and logs statistical information in the certification authority.

Security Server is for the general user, which provides security services, like applying, browsing certificate, downloading certificate revocation lists and certificate. The communication between security server and the user take secure channel, and does not require user authentication.

End Entity is the user of certificate, includes users, browsers and other secure application.

B. Certification Process of Railway Passenger and Freight Digital Certificate

Personal identity digital certificate authentication process

is shown in Fig. 3:

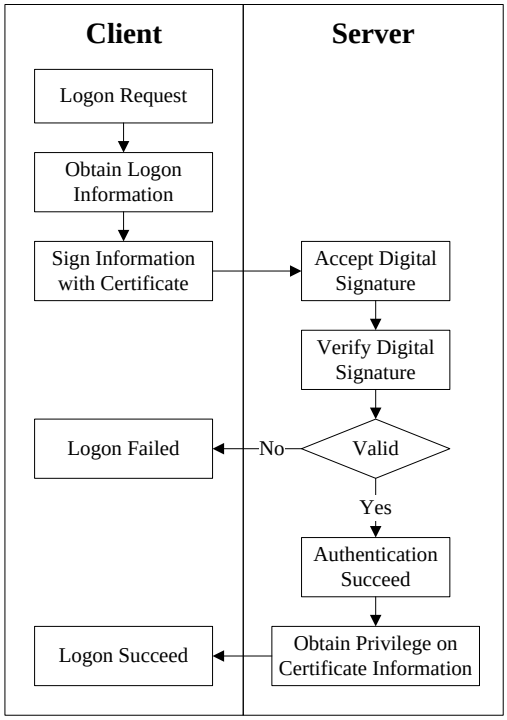

Fig. 3. Personal identity digital certificate authentication process.

1) Loading process

The basic requirements of password protection: [7]

1) Display the password in plaintext is prohibited; the password should be replaced by the same numbers of special characters.
2) The password should require complexity, and its length is at least six digits; it should prompt customers not to use a simple one when they are setting password.
3) It should force the users to change the password when they are first landing if there is an initial one.
4) It should have protection measures to prevent brute force password cracking, such as graphic code certification, the graphic code should be consist of numbers and letters, randomly generated, contain enough information about the interference; have a time limit to use, and can only be used once.

2) Loading control:

1) If the consecutive failed login time is more than 10 times, locking the user rights.
2) The session should be terminating when the user logouts or the browser page is closed, which ensures it cannot re-login by inputting address or typing the backspace button.

3) Certification process

1) A bi-directional authentication should be processed between server and client.
2) During the entire communication, certified communication lines should be kept secure connection status.
3) The system should be able to judge the idle state. When the idle is over a certain time, the current connection closes automatically, users must re-login to operation. [8]
4) It should ensure the root certificate of financial institutions WEB server is real and effective.

VI. The Combination of Railway Passenger and Freight Security Certificate and OTA

OTA which is the abbreviation for Open Travel Alliance provides sufficient guidance for companies to build systems which are highly interoperable with systems built by other companies. Apply OTA to railway passenger and freight E-commerce, makes interconnection of ticketing systems between different railway companies and railway or other means of transportation realized. The interaction of electronic information between the various systems follows the OTA message structure and norms, which provides technical foundation for multimodal transport between railway and other means of transportation and E-commerce. [9]

In addition to the functional specification related to business functions, OTA technical specification also defined non-functional technical specifications in the following technical requirements, including Session Management, Connection Management, Synchronous and Asynchronous Messaging, Payload Security, Transport Security, Information Integrity and Security, Authentication and Authorization, Security Strategy, Flow Control, etc. [10]

Based on the practice of China's high-speed railway passenger dedicated ticketing system, one after another normative railway ticketing system information interface has been specified start from the OTA standard 2010B. The High Speed Railway Research Center of Tsinghua University joins and dominates some of the designs. The Center makes a lot of contribution to many railway ticket system information interfaces independently and jointly, such as OTA_RailScheduleRQ/RS, OTA_RailPaymentRQ/RS, OTA_RailPriceRQ/RS , OTA_RailFareQuoteRQ/RS, and so on.

VII. Conclusion

The main purpose of the security certification of railway passenger and freight E-commerce is to certificate information in e-commerce transactions, confirm the identity of the message sender, verify the integrity of the information, and ensure the confidentiality of the user information and non-repudiation in the transaction process at the same time.

Railway passenger and freight is facing increasingly fierce competition in the market, relying on information technology to transform traditional transport enterprises, developing E-commerce system of railway passenger and freight, and improving transport efficiency and service levels of railway passenger and freight, has become the primary means to enhance market competitiveness. Information security of railway passenger and freight E-commerce provides effective protection for railway informatization.

Acknowledgement

The work is beneficial from the Research on E-Business Information Specification of Rail Passenger & Freight in China MOR (Ministry of Railway) 2011 annual research and

development program about the Application Research of Information Technology strongly.

REFERENCE

[1] C. Jiang, S. Yang, C. Liang, and Z. Chen, "The study of development strategies of Chineserailway e-business system," in *Proc. International Conference on Services Systems and Services Management*, pp. 809 - 813, 2005

[2] X. L. Sun, B. J. Wang, M. Gong, S. S. Ding, and A. Q. Tian, "Study on the Safety of High-Speed Trains under Crosswind," *AISS*, vol. 5, no. 1, pp. 582-588, 2013

[3] *Ministry of Railways, Railway Passenger and Freight E-commerce Standard*, Railway press, China, 2012

[4] X. Y. Li and H. S. Sun, "Research on security of e-Business for railway freight," *Railway Computer Application*, vol. 13, no. 11, pp. 45-47, 2004

[5] M. M. Xiao and S. F. Liu, "Architecture for Operation Management in Urban Railway System," *AISS*, vol. 3, no. 6, pp. 88-94, 2011

[6] H. Feng, "The Research on the payment authentication and security of the railway E—payment Platform," Master Thesis, Beijing Jiaotong University, 2010

[7] M. Hui, "Security and Privacy Protocol for Traffic Tracing," *IJACT*, vol. 5, no. 4, pp. 133-139, 2013

[8] C. J. Liu, D. M. Liu, Y. H. Li, M. Yang, and J. Zhang, "Construction of the electronic commerce security system based on Internet," *PACIIA 2009*, pp. 77-79, 2009

[9] F. Wang, H. B. Dong, C. Yang, K. F. Gao, and Y. W. Liang, "An Approach for Protecting Users' Relationships in the Process of Identifying Requestor's Right of Access in Online Social Networks," *AISS*, vol. 5, no. 3, pp. 347-354, 2013

[10] M. Vukmirovic, M. Szymczak, M. Gawinecki, M. Ganzha, and M. Paprzycki, "Designing new ways for selling airline tickets," *Informatica*, vol. 31, no. 1, pp. 93-104, March 2007

[11] A. Cieslik, M. Ganzha, and M. Paprzycki, "Utilizing open travel alliance-based ontology of golf in an agent-based travel support system," in *Proc. 9th International Conference on Artificial Intelligence and Soft Computing - ICAISC 2008*, pp. 1173-84, 2008

Xue Hu was born in Liaoning Province, China in 1990. Her major is software engineering. She graduated from Center for High-speed Railway Technology, Tsinghua University. Her research field is virtual reality simulation.

Yang Li was born in 1989, Inner Mongolia Province, China. She graduated from Center for High-speed Railway Technology, Tsinghua University, Her major is software engineering. Her research field is virtual reality simulation.