# Design and Implementation of Key Management System in IC Card Application for Public Transportation

Yang Xin[1, a], Du Ye[1,b] and Zhang DaWei[1,c]

[1]Institute of Computer and Information Technology, Beijing JiaoTong University, China

[a]yangxin-lb@163.com, [b]ydu@bjtu.edu.cn, [c]dwzhang@bjtu.edu.cn

**Keywords:** Key management system; symmetric key; asymmetric key; cryptography application

**Abstract.** Key management system deals with the key question for the entire process of key from produce to final destruction ,including system initialization, key generation, storage, distribution, renovation, destruction and more. The paper conducts research for public transportation IC card certification and transmission mechanism. Structuring and modularization are adopted in the design of general encrypt signature algorithm, moreover, a key management system with safety audit function has been proposed and realized. The test shows that the system can be used as an independent management services system with both symmetric key and asymmetric key to ensure safety. It can provide key management and service for the business system. Meanwhile, it can be used in the national urban public transport IC card electronic payment services widely.

## Introduction.

Key management system (KMS) is implemented by using the key encryption algorithm and the hardware encryption device to manage all kinds of key in business from the practical aspect of key usage. The purpose of this paper is to conduct research and design the technology of key management, analysis the logical hierarchy of key management system, system deployment structure, function and subsystem division and implement the design into real use.[1] There are five main features in this system. Firstly, this system satisfies the requirement of multi service key management; Secondly, the system supports the requirement of China financial integrated circuit card specifications (PBOC3.0) in key generation, transmission, issuing, key update, key management and service requirements. Besides, it issues security certificate in two level and support the cryptographic algorithm approval by State Cryptography Administration Office of Security Commercial Code Administration (OSCCA). It fulfills the general interface instruction of the transport IC card system. Furthermore, it has a perfect personnel certification, safety control, operation and maintenance monitoring and audit mechanism in the safety management. Last but not the least, the system can be used as an independent key management center as well as a connecting system which would supports related key service once it is connected with other data preparation system, card issuing system.

## System Analysis.

According to the requirements for key management in provincial level and city level, KMS should cover the entire key life cycle of the whole process from key generation, backup, recovery, transmission to destruction. [2]During the process of key production and transmission, the system support a variety of symmetric algorithm, digest algorithm and asymmetric algorithm, especially the OSCCA cryptographic algorithm. There are several functional requirements which are differentiated from other systems.

(1) Concerning the demands of key distribution of provincial level and city level, the symmetric key requires two-level key management system. The first level of key system should support single distribution of the Purchase Secure Access Module (PSAM) card and first-level primary key, and the second-level key system should support twice distribution of PSAM card, certificate request for card issuers and the receiving of second level key.

 

(2)Considering the different requirement in various cities for the key, it would be more convenient to expand the system and to meet the need of smart card project though using templates to develop the KMS, the key algorithm and its features in a flexible way. In this case, providing a benign flexibility and connectivity would offer a friendly interface for future card-distribution system, data-preparation system and personnel system.

**System Architecture.**

In order to meet the security request and functional need mentioned above, the system structure layout should satisfy the requirement of safe communication, the requirement from provincial level and the requirement from city level at the same time.

The card key management system utilizes three layers of architecture, which are the system platform layer, data layer and the operating environment layer.

First of all, the key application system is provided by the KMS (such as: card issuing agencies, data-preparation system, CA organization, etc.), it is mainly for the customized city-level services. Specifically, system platform layer is composed of key generation system, key management service system, security authentication system and security audit system. It is the core of the KMS, including symmetric key management and asymmetric key management, certificate management module, etc. Besides, data layer is a KMS database. The Oracle database is adopted for security consideration,which would provide information, data and other resources for the KMS. Finally, the operating environment layer offers a safe and stable operation support for the data layer and business platform layer, which consists of the hardware environment, the basic software environment, and the network security environment.

**System Design.**

There are four subsystems in this system, including key generation subsystem, key service subsystem, security authentication subsystem and audit certification subsystem.

In key generation subsystem, operator uses the parameters configuration function to complete the requirements of key generation.[3] Parameters configuration includes the configuration of encryption, key algorithm, key pool, key generation strategy and so on. The encryption configuration contains IP address, port number of service and other parameters. Key algorithm configuration includes the supported symmetric type (SM1, SM4, DES, etc.) and asymmetric type (SM2, RSA, etc.) of cryptographic algorithms. The key generation strategy includes manual generation and automatic generation strategy. Symmetric key and asymmetric key can be generated randomly according to the algorithm type. In the system, physical noise generator (e.g. WNG4/8) is primarily used to generate random numbers. These numbers can be adopted as the key material to generate key once they passed the random number quality test.

As for the key service subsystem, it not only provides management of the entire key life cycle, but also supports extended application and offers digital certificate management function. [4]When distributing the key, it uses input and output processes to realize the transportation of key from higher level to lower level. The key card which saves the output key and the control card which stores privilege control key are served as the delivery carriers. The superior key management center outputs the key to key card and delivers it off-line to the secondary key management center with initialized control card. Then, the secondary key management center uses control card and key card to export the key and imports it into relevant local cryptogram equipment to store it in corresponding position.

**System Implementation.**

The system applies B/S structure and SpringMVC model which is combined with Hibernate technology. According to the concept of using layered service to support business, the KMS is divided into View, Controller and Manager.

**Process of Certification Issuing.** Following "Technical specification for urban public transport IC card", the KMS system consists of two levels of key management system, which is ministry key system and the card issuer key system. Ministry key system is responsible for the management of financial certificate, which include the generation of root certificate and self-issue, certificate issued, ministry key's generation, maintenance, and distribution.[5] The key management system of card issuing should be established by card issuing institute, and this system is responsible for receiving the ministry root certificate, the application and reception for card issuer certificate, the import of the ministry key, and the generation and maintenance of exclusive key of card issuer.

The generation of asymmetric keys and the certificate issue as is shown in following picture:

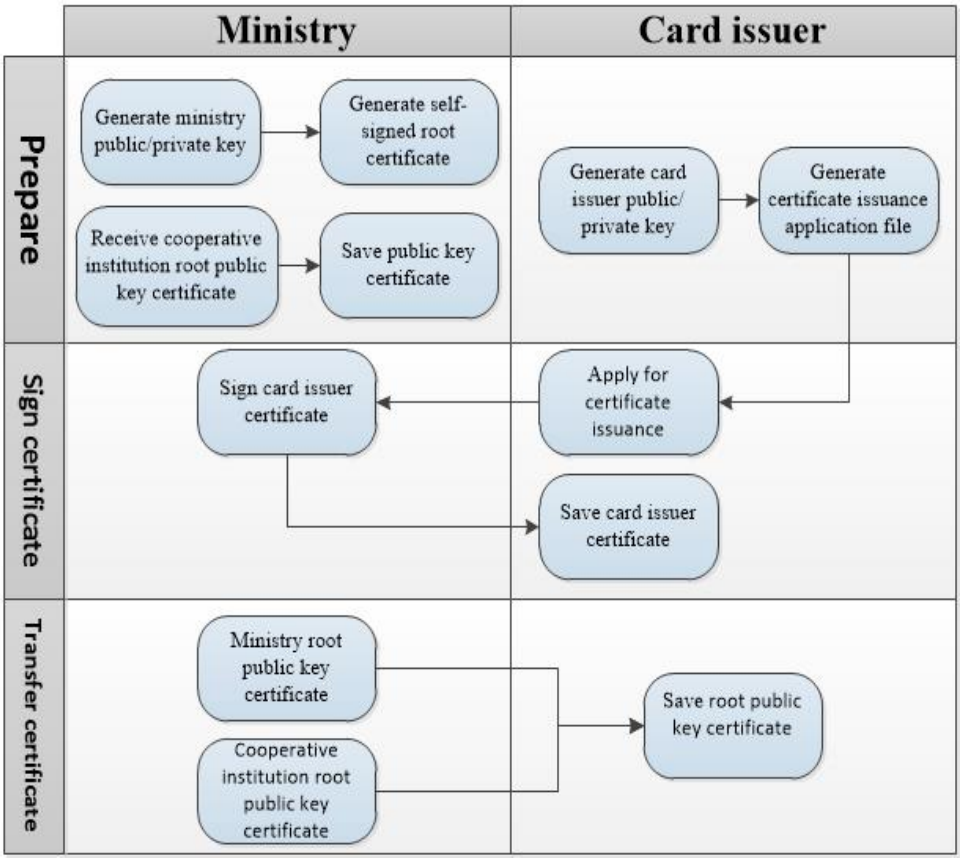


Fig. 1 Certificate Issuance Process

Specific process is as follows:

(1)The ministry key management center generates a set of different lengths of ministry authentication and public/private key pairs (authentication for center of root public-key) and saves them;

(2)Card issuer generates an appropriate length of public/private key pairs for each category of cards and saves them;

(3)Card issuer submits a certificate request file with a signature by its public key to ministry authentication center;

(4)Through the private key, ministry authentication center signs the card issuer public key, then generates the card issuer public key certificate, and sends it to card issuer for saving;

(5)Card issuer randomly generates a pair of public and private keys for each transportation IC card, and uses card issuer private key to sign IC card public key and some static data, then generates transportation IC card public key certificate and signatured static application data;

(6)Card issuer writes the data of card issuer public key certificate, transportation IC card public key certificate, signatured static application data and transportation IC card private key into transportation IC chip;

(7)Ministry authentication center distributes its public key to each acquirer through the suitable way. Acquirer downloads the ministry authentication center public key to its terminal so as to authenticate transportation IC card by the offline data when dealing.

**Security Test.** In order to guarantee KMS's key security, we need to conduct a comprehensive security testing after the implementation of the system. The security test is divided into three categories.

The first is pressure security testing during the long-time test of randomly generating key . In this test, the system should run normally and the cipher machine can generate related key according to user requirements. After two days of testing, the system has no anomaly.

The second is access security testing. Operator and administrator should operate according to their respective permission. [6]Once they access unauthorized interface or operation, because of using AOP technology, the system will determine the permission at controller layer. If the permission does not satisfy the requirements, system will refuse to do related operations. The third is illegal invasion testing to see if we can directly access the password service layer and cipher machine through network. Due to cipher machine and password service layer have white-list related strategies, the visitors who do not access from the specified network will be rejected, so the security of system is protected.

## Conclusion

The paper conducts research on the design and implementation of a KMS to solve problems that the existing systems fail to unify management in symmetric and asymmetric services, and the application of OSCCA cryptographic algorithm is insufficient in business services. In the life cycle of key generation, storage, distribution and more, the system can fully use efficient communication services and strong security encryption device through a variety of encryption and signature algorithm such as RSA, DES, AES and OSCCA cryptographic algorithm to provide users with extended functions. Meanwhile, the strict issuing processes of the certificate ensure the security of KMS which can effectively solve the problem of the application of public transport IC cards. In conclusion, experimental application indicates that this system not only provides a comprehensive and efficient solution for key management, but also supplies a good basis for the national IC cards in China.

## Acknowledgements

This work is supported by the Beijing Higher Education Young Elite Teacher Project (project No. YETP0548), the Fundamental Research Funds for the Central Universities (project No.2014JBM030). The authors are grateful for the anonymous reviewers who made constructive comments.

## References

[1] Rafaeli S, Hutchison D. A survey of key management for secure group communication.[J]. Acm Computing Surveys, 2003, 35(3):309--329.

[2]Andrew Nash, William Duane, Celia Joseph, Derek Brink. PKI Implementing and Managing E-Security. McGraw - Hill Edueation.2001.

[3] RFC3280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002.

[4] Garcia E, Colorado C A. System and method for communicating with a key management system: US, US8667267 B1[P]. 2012.

[5]Ray Hunt. PKI and Digital Certification Infrastructure. Proceedings of the 9th IEEE International Conference on Networks. 200l: 234 – 239

[6] Daubignard M, Lubicz D, Steel G. A Secure Key Management Interface with Asymmetric Cryptography[J]. Lecture Notes in Computer Science, 2014:63-82.