International Journal of Innovative Research in Electronics and Communications (IJIREC)
Volume 2, Issue 6, August 2015, PP 29-31
ISSN 2349-4042 (Print) & ISSN 2349-4050 (Online)
www.arcjournals.org

PKI Technology for Data Encryption

ZHU Zhenfang

School of Information Science and Electric Engineering, Shandong Jiaotong University, Jinan, China
zhuzhfyt@163.com

Abstract: *These PKI is a kind of follow the standard use of public key encryption technology for the development of e-commerce to provide a secure foundation platform technology and specifications. The application of digital certificates is under the network environment to solve the problem such as identity authentication, access control, and information protection. This thesis mainly studied the part of the problem, this paper introduced the basic knowledge of cryptography and PKI theory foundation and basic system, of several common PKI trust model had carried on the detailed introduction, designed the distributed network environment, interconnection security platform of authentication and information encryption module.*

Keywords: *Public Key Infrastructure; Digital Signature; Digital Certificate; RC4 Algorithm; Security Support Platform*

1. Introduction

With the development trend to network economic era of global economy, e-commerce becomes the major method. Its application reduces the trade cost to the great extent, increases trade activity opportunity, makes trade procedure simpler, and significantly improves the efficiency of network commerce trade. However, direct contact between people reduces under network environment, so the trust relationship by verification with electric method becomes a crucial link.

PKI (public key infrastructure) can be well applied in the encryption of trade transaction. Its principle is to generate generation certificate by using the public key for certificate management and binding public key and identification letter with certificate authority (CA). Users can use this certificate as the evidence for identity. Under this condition, we will encrypt all the digital information and give signature, so security problems of file confidentiality, authenticity, integrity, non-repudiation, and access control occurring in e-commercial application can be well solved.

2. PKI foundation

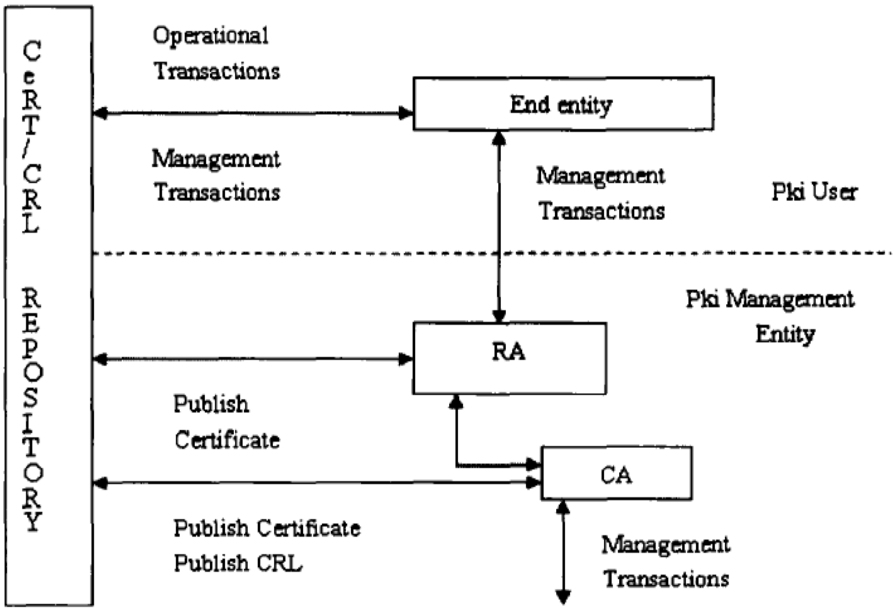

Fig1. *PKXI standard*

The basic definition of PKI is very simple. As a new measure to ensure the network information security, PKI includes public-key cipher technology, digital certificate, certificate authority (CA) and security measures about public key [2]. As a basic infrastructure, PKI technology can ensure the security of network transaction by applying public-key technology. The security of network transaction and payment code is realized by PKI technology.

PKI includes five components in effects as shown in Figure 1 according to PKXI standard:

3. DATA ENCRYPTION DESIGN FOR SECURITY SUPPORT PLATFORM

3.1 Demand Analysis

By data encryption, a measure to protect information in the security support platform, it can be ensured that the information cannot be used when the information is in authorized use [3]. In other words, data encryption aims at protecting firstly, the ownership and use right of information resources which are publicly known, and secondly, sensitive information, such as state secrets and commercial secrets which can only be grasped by people in corresponding level with confidentiality. Such sensitive information must be encrypted to prevent illegal users from stealing because the consequence of disclosure is severe.

According to above analysis, customers involved in actual application are not familiar with encryption technology, so the requirements for data encryption design are as follows:

(1) Certain security. Security means stealing information costs larger than encryption, instead of being unable to steal the information.

(2) Good variability of information encryption. There is no specific format requirement for data to be encrypted that is, data file in any format can be encrypted by flexibly changing encryption key.

(3) Convenient use. The encryption of data information is public, rather than in secret, so it certainly may affect the normal use by users. Therefore, the encryption speed is significant to PKI.

3.2 Selection of encryption algorithm

With the development of cryptology, the method of data encryption also updates. In general, DES encryption algorithm is always used in data encryption, and the transformations of DES are very safe at present. However, the encryption to data information in this work obtains initial information with the efficiency of user access that is, the available quantity of data information in the shortest period. Therefore, the primary condition must be the speed of encryption and decryption. After comprehensive analysis on security of data encryption, it is decided to take the algorithm of sequential cipher, RC4 as the algorithm for information encryption. Involving the secret key transmission between two communication parties, mainstream algorithm RSA is selected for secret key encryption.

3.3 Design of mixed encryption system

There are two algorithms, including RSA and DES encryption and decryption algorithm. With the increasing development of computer system ability, the security of DES becomes weaker than that when it appears, so there are endless cases of DES decryption by retrospect. An actual machine can decrypt DES in a few days which makes people think that they cannot be dependent on the DES as the only way to ensure DES security [6]. Compared with DES, the security of RSA is relatively high. There are also some cases of RSA decryption, but it costs relatively large (compared with DES). Moreover, the secret key of RSA updates at present, which means that the difficulty to decrypt RSA also increases.

In RSA encryption algorithm, RSA encryption explicit term will be limited by the length of secret key. In other words, the term length of RSA is limited, while the actual term length may be larger than the encryption length, so we have to give up RSA encryption because DES encryption is unlimited.

Given above two points (personal points), separate use of DES or RSA encryption cannot satisfy with the actual demand, so the combination of RSA and DES encryption is used to realize the data encryption.

3.4 Realization of analog simulation

If two communication parties are interconnected after identity authentication, both parties will obtain public key certificate and know the RSA key of each other. Therefore, safe communication can be realized with combined encryption. For sender A, the system will randomly generate an encryption secret key with corresponding term, and the summary user of file can decide if the calculation is necessary on his own. Next, RSA encryption is conducted for RC4 secret key with the public key of sender. At last, these two parts of cryptograph will be combined with an info-head to form a new file which will be sent to receiver. In aspect of service terminal, digital certificate and explicit term can all be pretreated by managing encryption key [7]. For receiver B that is, the decryption, however, RSA secret key is extracted by secret key certificate to do RSA decryption and obtain RC4 secret key before obtaining explicit term with RC4 algorithm. If the integrity needs to be verified, the summary should be obtained by calculation with the public key of sender. At the same time, the summary of explicit term obtained by decryption should be calculated. It can be judged if the information is manipulated by comparing these two summaries [8].

4. Conclusions and Prospect

In the age of rapid informationization, science and technology are updating at every moment. Because of the replacement of old technology with new technology, our life becomes increasingly modern. In early stage, we used RSA algorithm to ensure the information security and protect private data. However, this technology cannot satisfy with our demands anymore, so new technologies, PKI emerges, meaning that the security of data information enters into a new stage.

Acknowledgments

National Natural Science Foundation (61373148), National Social Science Fund (12BXW040); Shandong Province Natural Science Foundation (ZR2012FM038, ZR2011FM030); Shandong Province Outstanding Young Scientist Award Fund (BS2013DX033), Science Foundation of Ministry of Education of China(14YJC860042).

References

[1] Wade Trappe Lawrence C.Washington. introduction to cryptography [M]. Beijing: People's Posts and Telecommunications Press (2004-6-1).

[2] PKI CA[M]. Zhensheng. The certification bodies and the electronic industry press set key (2002).

[3] Bruce Schneier. applied cryptography [M]. Wu Shizhong, Zhu Shixiong, Zhang Wenzheng, et al. Mechanical Industry Press (2004).

[4] Lu Kaicheng. Computer cryptography [M]. Tsinghua University press (1998).

[5] Hao Yu, Yu Jianping, Wu China. Tolerance intrusion of RSA signature step by step scheme and its application in ca. Computer science, 2004,31 (11): 83-85.

[6] IT system security white paper.Http://www-900.ibm.com/cn/support/guide/whitebooks/Security /security.shtml.

[7] Bai Xiaomin, Jiang Yanhuang, Yang Xuejun. Digital signature technology and its development trends. Computer application research, 2000,11 (9): 1-3.

[8] St Denis Simon, Johnson. [8]Tom programmer cryptography [M]. Shen Xiaobin translation. Mechanical Industry Press (2007).

[9] Technological Infrastructure for PKI and Digital Certification. Computer Communications [J] Rayhunt., 2001, (24): 1460-1471.

[10] Yang Bo. Now [M]. Tsinghua University press, 2007

Author's Biography

ZHU Zhenfang, PhD, lecturer, he was born in 1980, Linyi City, Shandong Province. He obtained Ph.D. in management engineering and industrial engineering at the Shandong Normal University in 2012, his main research fields including the security of network information, network information filtering, information processing etc.. The authors present the lecturer at the Shandong Jiaotong University, published more than 30 papers over the year.