The Application of Cryptography in PKI

Wenjie Zheng

Power University Baoding, Baoding 071000, China

2893687936@qq.com

Abstract

The article first briefly describes the PKI architecture, and then analyzes the two-dimensional code security algorithm as an example. The article is based on PKI architecture of two-dimensional code, the algorithm is divided into three modules: key management module, two-dimensional code production module, two-dimensional code recognition module.

Keywords

PKI, cryptography.

1. Introduction

PKI is essentially a set of basic technologies and specifications for maintaining network security, including digital signature services and public key encryption. The system is a PKI system. The application of PKI in electronic information is mainly to ensure the safety of the network operating environment used by the user. It is reliable, the safety technology and safety measures it uses are more, such as the digital certificate "public key technology" certificate issuing agency, etc. To a great extent, the confidentiality and integrity of various types of data transmitted in the network during the operation are classified as confidential and complete. It is the best guarantee for the network society that is recognized in the field of electronic information security protection.

2. Framework of PKI

(1) PKI security policy: It is the definition of guidelines and cryptographic system application principles and methods for information security.

(2) Certificate Authority CA: It mainly manages the life cycle of public keys and is the trust foundation of PKI. The main functions of the CA include: issuance of certificates, provision of valid term of use of certificates, timely release of certificate revocation list CRL, and so on.

(3) Registration Authority RA: Reads the user's identity, completes the user identity authentication, and then transmits the certificate request to the CA to provide the interface between the CA and the user. The main function of the CA is to collect and authenticate the customer's identity information submitted to the CA for digital certificates. And these applicants do not refer to individuals only, but also include government agencies, businesses or other groups. The registration authority is only responsible for the user qualification review, not the issuance of the certificate.

(4) Certificate issuance system: The main function is the issuance of a qualified customer certificate. Among them, customers who passed the qualification examination can either directly use the Internet to download online, or they can apply for the corresponding organization to send points to complete the certificate collection.

3. PKI-based QR code security model algorithm

The two-dimensional code security algorithm studied in this paper is based on the application background of e-commerce. In the algorithm design process, the three main steps are considered.[2]

Step one: Solve the key distribution and management, and review the certificate application.

Step 2: The e-commerce provider applies for keys and certificates through the CA center, and also provides service functions to users.

Step 3: When the user obtains the e-commerce service, he can also obtain the CA center's key for security verification.

This algorithm model uses the structural design concept, which not only defines the roles of different modules before the role and the problems that need to be solved, but also closely relates the relationship between different modules. By using the topological, top-down, divide-and-conquer concept of the security model, it is possible to effectively decompose a complex engineering problem into a single subsystem that is easy to control and handle, and facilitates management personnel's optimization and maintenance of the system.

The algorithm is based on the PKI public key system and can be divided into three modules: key management module, two-dimensional code production module, two-dimensional code identification module; these three modules correspond to three different roles: CA center, service delivery Business, users; as shown in the QR code security application role diagram.

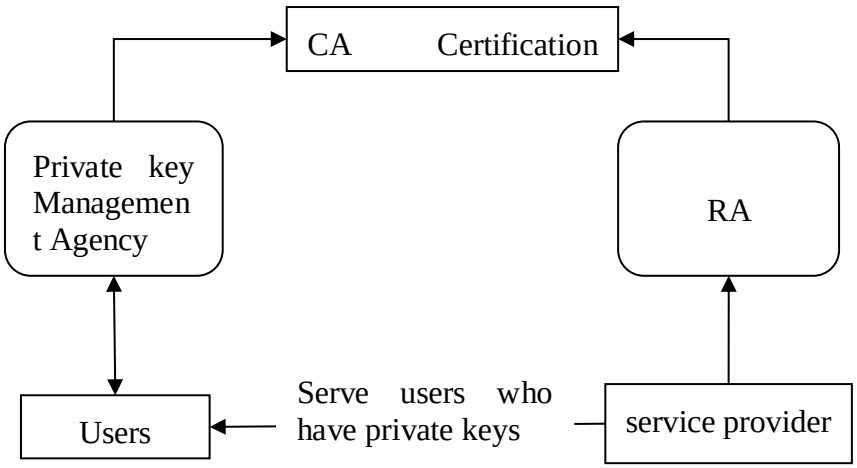

Fig. 1 QR code security application system role diagram

The key management module in the above algorithm model is the core module of the entire two-dimensional code security application system. In the algorithm design, the system uses the RSA key algorithm for encryption. The difference from the traditional RSA encryption algorithm is that the system is distributed to users. The "private key" is used to encrypt the two-dimensional code, and the "public key" stored in the system is used to decrypt the two-dimensional code. Compared with the traditional asymmetric public key system, private key encryption can solve the problem of data encryption, that is, data security; public key decryption can solve the problem of decryption and identity authentication, that is, authenticity and identification problems. This solution can not only guarantee security, but also solve problems such as identity authentication.

(1) Key Management Module

The key management module is mainly controlled by the CA center. This module is mainly responsible for key production and management. This module uses asymmetric key encryption, and public and private keys are paired. The user's private key is responsible for encrypting the two-dimensional code, and the CA Center uses the public key for decryption.

(2) QR code generation module

The two-dimensional code generation module is mainly responsible for image generation of the two-dimensional code, and performs integrity verification on the original information during the generation process, and then uses the private key of the user in the key management module for encryption.

(3) QR code recognition module

The two-dimensional code identification module is mainly responsible for reading the two-dimensional code image code, including: pattern recognition of the image, image processing technology, positioning and correction of the two-dimensional code, error correction and decryption

of the two-dimensional code, and verification of the digital signature Confirm the validity of the QR code.

4. Algorithm model function module analysis

With the increasing development of the Internet, there are various forms of e-commerce. The paper uses online and offline (OTO) e-commerce to conduct experimental simulations. In this paper design, the two-dimensional code management platform acts as a CA role to uniformly generate and manage keys, and an e-commerce platform generates and generates two-dimensional codes. Finally, it is sent to the consumers. When the consumers get the QR code on the line, they can go to the offline physical store and use the two-dimensional code to scan the terminal to determine its legitimacy. The system two-dimensional code security platform system shown in Figure 2 and Figure 3. [3]

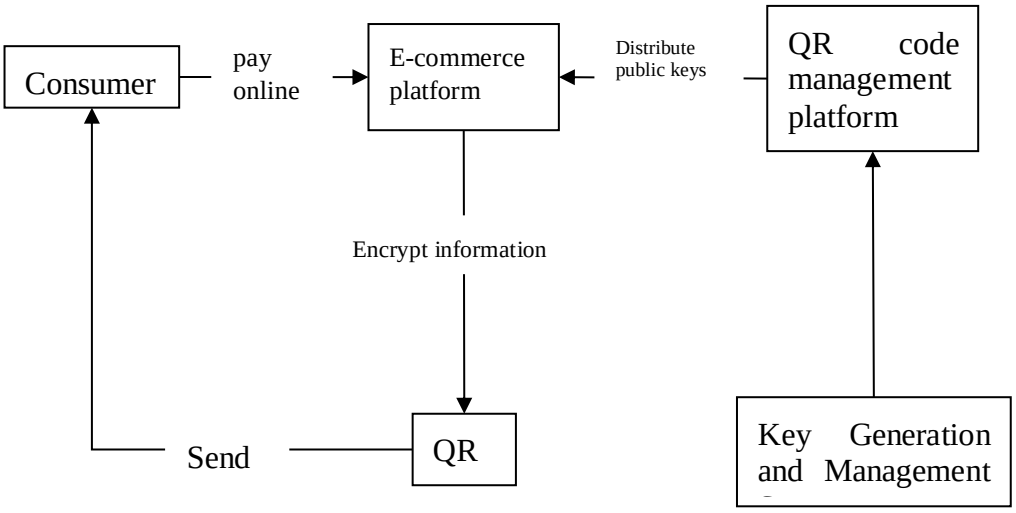

Fig. 2 Security System Platform Online Diagram

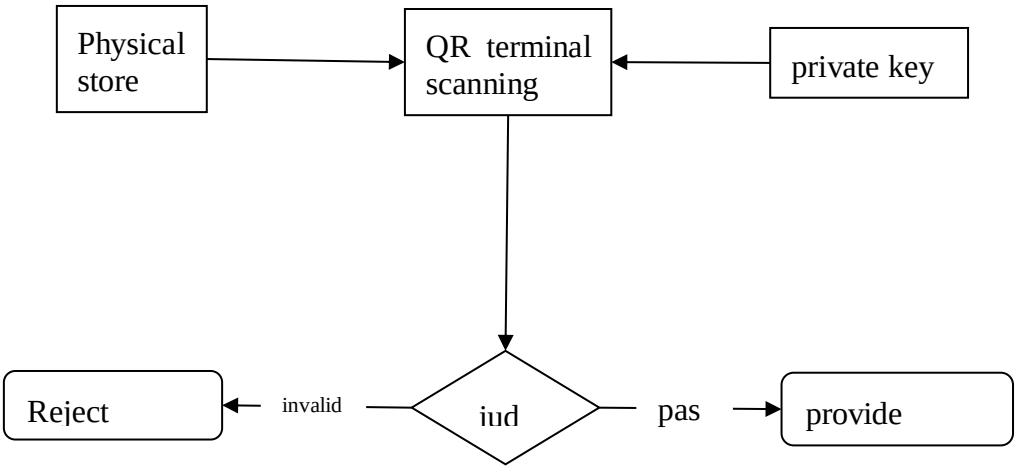

Fig. 3 Security system platform offline mode diagram

(1) The e-commerce platform encrypts consumer and product related information through a key management server and sends the encrypted two-dimensional code to consumers.

(2) Consumers use the QR code to verify the legitimacy of the physical store, when the two-dimensional code mobile terminal reads the information and links to the database of the two-dimensional code management platform, this time through the database comparison judgment.

(3) If the query is successful, the public key is sent to the key management system, the public key is used for decryption, and the decryption succeeds in determining the legitimacy of the identity. The user can then extract the goods, and vice versa.

5. Conclusion

With the rapid development of information technology, people are increasingly demanding information on the Internet. Whether it is HTTPS, SET, or PKI technology, it is to meet people's needs. As early as Caesar's time, there was Caesar's code, the seeds of cryptography began to germinate since then, and in the age of the Internet, the study of cryptography presented a phenomenon of prosperity, which has important significance for individuals and even the information life of the country.

Early classical cryptography was able to perform simple encryption. With the further study of information theory, these cryptographs are no longer able to withstand the attacks of the crackers. The generation of symmetric cryptosystems increases the strength of encryption and satisfies the encryption requirements well. However, there are problems in the distribution and transmission of secret keys. The public-key cryptography that was born later can solve this problem and assist in the implementation of symmetric secret keys. transmission. Based on this, digital envelope technology has been produced. In addition, public key cryptosystems can also be applied to digital signatures, message authentication, and so on.

The creation of a large amount of information encryption technology makes it possible to guarantee the security of information, but the promotion of technology is facing new challenges. PKI technology is to solve the key distribution, management, loss and other issues. SET protocol is the use of dual signatures in the electronic transaction process to achieve the isolation of ordering information and payment information, HTTPS protocol is to achieve secure network information transmission. The generation of these technologies stems from the increasingly stringent demand of people for information security. On the one hand, they rely on the continuous development of cryptography to provide technical support.

References

[1] Shi Wenjie. Research on security of two-dimensional code based on PKI technology [D]. Anhui University of Technology, 2017.

[2] Zhang Hao. Discussion on the Application of PKI in Electronic Information Security [J]. Building Materials and Decoration, 2017, (08): 154-155.

[3] Lin Yi, Jing Jiwu, Zhang Qionglu, Wang Zhan. A Review of Recent Researches on PKI Technology[J]. Chinese Journal of Cryptography, 2015, 2(06): 487-496.