The Mobile payment based on public-key security technology

IOP Conf. Series: Journal of Physics: Conf. Series **1187** (2019) 052010 doi:10.1088/1742-6596/1187/5/052010

The Mobile payment based on public-key security technology

Jiabin Sun[a], Nan Zhang[b]

International School, Beijing University of Posts and Telecommunications, Beijing 100876, China

[a]sunjiabin@bupt.edu.cn

[b]2015212939@bupt.edu.cn

Abstract This paper mainly concentrates on data security technology applied on the mobile payment application in China. The widely used technology of public-key encryption will be introduced in this paper and it also includes the mobile payment system mode applied in Chinese mobile payment application. And it aims at how the technology serves for different business to meet the users' requirement, and how the technology adjusts to different market requirement.

1.Introduction

With great convenience and low cost, mobile payment has become an essential part of e-commerce. And therefore, it is particularly important to ensure the information security during the paying process. As a result, it is very necessary to conduct a research on efficient security mechanisms for mobile payment, and on the relationship between the security mechanisms and the e-commerce business mode. With these considerations, this paper will demonstrate the issue from the following aspects:

First, a general theoretic research is conducted for the Mobile Payment System (MPS), including operation mode, and structure. Second, security mechanism of MPS is studied, including encryption technology, the comparison of symmetric and asymmetric encryption, and authentication method. Then the paper will focus on one of the most commonly used MPS in China, Alipay, and also the popular digital currency. By analyzing the differences of the two application, this research will try to find out how the technology adjusts to the market requirement.

2.Mobile payment system

2.1.Operation Mode

There are three main operation mode, distinguished by the different business operation entity: 1) mobile operators 2) banks 3) third-party service provider [2].

When the mobile operator acts as the main body of the mobile payment platform, the mobile operator will use the mobile phone number as the account, the user's mobile payment transaction costs the department deducts from the user's credit account. The mobile payment service with the mobile operator as the main body has the characteristic that there is no need for bank participation, and it is impossible to invoice the non-calling business.

When bank plays the main role as the main body of operation, it interconnects with the mobile communication network through a dedicated line, and binds the bank account to the mobile account. Banks provide users with trading platforms and payment channels, while mobile operators only provide information channels for banks and users, and do not participate in the payment process. At present,

most of Chinese business bank provides mobile banking, and operates their own mobile payment platforms.

The mobile payment service with the bank as the main operation has the following characteristics: each bank can only provide the use services of its own bank, and the mobile payment services cannot be interconnected between banks [2].

Payment service provider or mobile payment platform operator is the third independent of banks and mobile operator and it is also a bridge and link between mobile operators, banks and merchants. Through the operator of the trading platform, users can easily realize the mobile payment service across banks. The third party service provider is now playing a role of merging users and banks as users can access to multiple bank accounts on third party service provider, such as Alipay and Wechat [2].

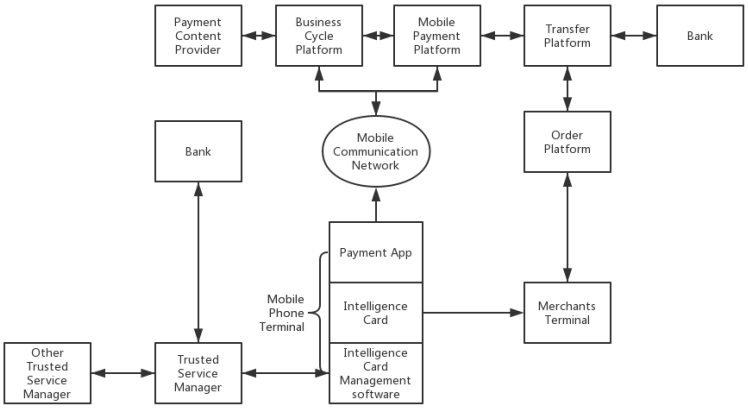

Figure 1. Flow chart of the mobile payment process [1]

2.2.Structure

The Mobile payment system (MPS) is consists of two parts: PA (Mobile Payment Agent) and MPP (Mobile Payment Platform) and they are connected by digital data network [2]. MPA is responsible for the management, fee-counting, and communication in nation-wide scale, connected with national business operation support system (BOSS); as MPP is responsible for the management, fee-counting, and communication in the local scale, connected with service providers. The UASS (Unified Account Service System) in BOSS provides unified management of the user accounts nation-wide. Users can attach their mobile phone number to their mobile payment account and also to their bank account [2].

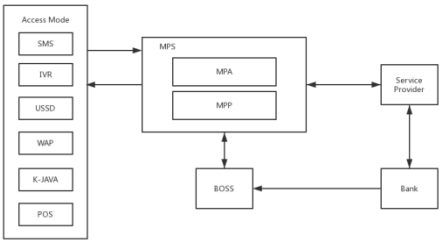

Figure 2. Structure of MPS [2]

3.Security mechanism of mobile payment system

3.1.Encryption technology

3.1.1.Symmetric encryption

Symmetric encryption uses a shared key (symmetric) to encrypt. That means the sender and the receiver hold the same key to encrypt and decrypt the message in the communication.

Key should be exchanged between the communicating entities before the transmission of data [3]. For the encryption process, exchanging keys is important. Weak and short keys can be easily attacked as compared to longer keys which are more difficult to break [3]. Symmetric key encryption algorithms are still widely used as powerful techniques in insecure communication channel [3].

The DES (Data Encryption Standard) is a commonly used symmetric encryption. DES was the first block cipher which was designed by IBM and it was adopted by national bureau of standard in 1977. DES algorithms take 64 bits plaintext as an input and transform it into 64 bits cipher text as output. The key length of DES is also 64 bits. DES is called a complex block cipher as it has 16 blocks of complex round ciphers and each block itself has a complex function [3].

3.1.2.Public-key encryption

Public-key encryption is asymmetric encryption because the sender and receiver are not using the same key to encrypt and decrypt. There are two types of keys used in public-key encryption, the public key and the private key.

The RSA algorithm is the one of the most commonly used public-key encryption. The algorithm uses two keys, the private key and the public key for encryption and decryption. The sender encrypts the message with the receiver's public key, which is known by everyone, and then the receiver decrypt the message with the private key which is only known by the receiver. In this way, the stand-in attack will be efficiently prevented, that even the attacker captures the message in the middle of the traffic, there is no way for the attacker to decrypt the message since the private of the receiver is needed.

The encryption process can be described as followed:1) Select two large prime numbers p, q; 2)Calculate $n=p*q$; 3) Calculate $\phi(n)=(n-1)(q-1)$; 4)Select integer e, such that $\gcd(\phi(n),e)=1$ and $1<e<\phi(n)$; 5)Let $d=k*e^{-1} \bmod \phi(n)$ $(k=1,2,3,...)$; 6)Public key is $k_u=\{e,n\}$, and private is $k_r=\{d,n\}$

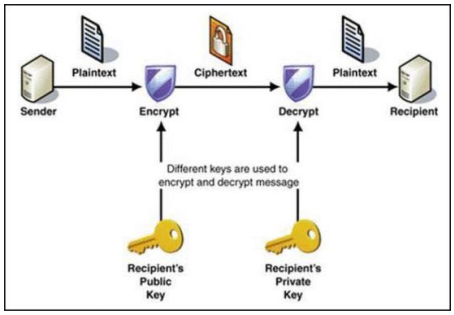

Figure 3. Process model of asymmetric key cryptography [3]

3.1.3. Comparison between symmetric encryption and public-key encryption

In general, there several differences between symmetric and public-key encryption. Symmetric encryption requires only one shared key while public-key encryption requires two secret keys, the public key and the private key. And as for only one key is required, symmetric encryption has better operation speed than public-key encryption but lower security level. Although public-key encryption has the advantage of security, the calculation of large prime numbers also increase complexity of the algorithm.

Table 1. Comparing the two different encryption method

Features	Symmetric encryption	Public-key encryption
Number of keys	1	2
Speed	Fast	Slow
Security	Low	High
Complexity	Low	High

3.2Authentication

3.2.1Digital Signature

Digital signature is an alphabetic string obtained through processing the transmitted text by a Hash, with the purpose of verify the source of text and confirm whether the text is undergoing changes [4].

To ensure the availability of digital signature, PKI (Public Key Infrastructure) is often used. It follows the standard public key encryption technology and offers a full set of security assurance infrastructure for sectors like e-commerce, e-government, e-banking and on-line banking securities [4].

Data signature technology can ensure that: information cannot be known by other sides except the senders and receivers; information during transmission will not be tampered with; the recipient is able to confirm the identity of the sender; sender information for their own cannot be denied. Digital signature uses public key cryptosystem, that is, it uses a pair of matching asymmetric keys to achieve the encryption and decryption, signature and verification at the same time [5].

The digital signature for a message is generated in two steps:1) generating a message digest which is a summary of the message using hash algorithms 2) encrypt the message digest with the sender's private key.

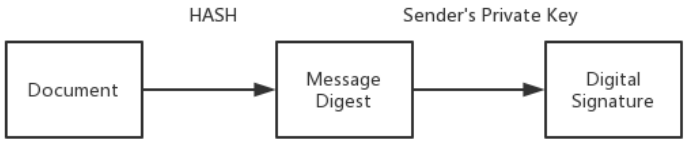

Figure 4. Digital Signature [5]

The digital signature is attached to the message, and sent to the receiver. The receiver then does the following: 1) Using the sender's public key, decrypt the digital signature to obtain the message digest generated by the sender. 2) Uses the same message digest algorithm used by the sender to generate a message digest of the received message. 3) Compares both message digests (the one sent by the sender as a digital signature, and the one generated by the receiver) [5]. If they are not exactly the same, the message has been tampered with by a third party. It is sure that the digital signature was sent by the sender because the message digest is encrypted by the sender's private key, so the receiver can decrypt it with the sender's public key, and also with the private key, the receiver is certain about the sender's identity.

3.2.2Certificate Authority

CA (Certificate Authority) is a trusted authority in a network that issues and manages security credentials and public keys for message encryption. As part of a PKI, a CA checks with a registration authority to verify information provided by the requester of a digital certificate. If the RA (Registration Authorities) verifies the requestor's information, the CA can issue a digital certificate. Indeed, the CA is responsible for the distribution and revocation of the certificate. Depending on the PKI implementation, the certificate might include the owner's public key, the expiration date of the certificate, the owner's name, and other information about the public key owner [6].

3.3Firewall

A firewall protects a local system/network from network-based security threats and at the same time allows access to the outside world. In most cases, firewall is required since it is difficult to equip every single device with strong security features. Usually, the firewall is inserted between the premises network and the Internet and it establishes a controlled link and security wall between the premises and the Internet.

4.Application of public-key technology in different business mode

4.1.Scanning-code payment

4.1.1.Security mechanism of QR Code

QR Code is an array of bits that can be used to store information. Information embedded in QR Code can be secured using various methods such as TTJSA algorithm, SD-EQR, hash function, reversible data hiding, steganography, histogram, symmetric encryption, asymmetric encryption, Reed-Solomon method, Signed QR Code (SQR Code), etc. [7].QR Code has its core structure (shown in Fig. 5). The encrypting and decrypting of the QR code relies on the encoding region of the code [8].

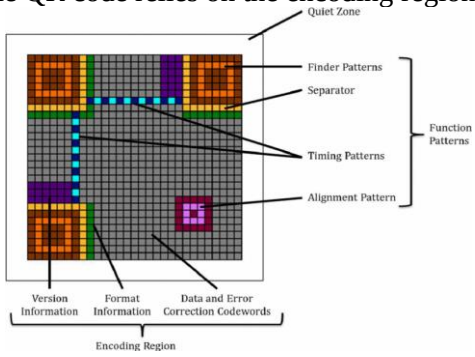

Figure 5. QR Code Structure [8]

If QR Code is dirty or damage, it does not matter because QR Code has error correction capability [7]. The QR code achieves powerful error-correction capability by using Reed-Solomon codes, a widely used mathematical error-correction method,and four levels of error correction(L-7%, M-15%, Q-25%, H-30%) are available[8]. Data can be restored even if the symbol is partially dirty or damaged. As long as the Finder patterns are not masked and no more than 30% of the code is hided, then the data can be restored [7].

4.1.2.QR Code in mobile payment

The QR Code encryption through PKI in mobile payment system can be divided into the following seven steps: 1)the user gives user ID; 2) the merchant receive user ID;3) the merchant request public key to third party; 4)the third party generate public key and private key based ID;5) the third party authenticate and receive private key; 6)the merchant generates QR code uses public key; 7) the user scan QR code ,decrypt using private key, and verify received message[7].

In the case of Alipay in China, there are three modes of QR code that are commonly used in real business scenario: 1) the identity code 2) the receiving code 3) the paying code. As for the identity code, what is encoded in the code is a URL with an encrypted identity message, and this information is unchanged and cannot be seen. For the receiving code, what is encoded in the QR code is also a URL (a different API) with an encrypted message, and this information is also unchanged and cannot be seen. For the paying code, it is not a URL that is encoded in the QR code, instead, a string of numbers is encoded, and this string of number changes every minute. From the QR code model below it is clear that the string of number that encoded in the QR code is the public key that is generated by the third party used in every transaction. This could explain why merchants using Alipay can have a permanent QR code for receiving money, because the information encoded in the QR code is unchanged, and the code itself does not need to be changed. For different payment application, the difference between their QR codes is the URLs and APIs that encoded in the QR code.

For the users of Alipay, what they require is both safety and convenience for their payment, and therefore, Alipay uses QR code technology through PKI to encode and encrypt the users' data to ensure the payment safety and enhance the user experience.

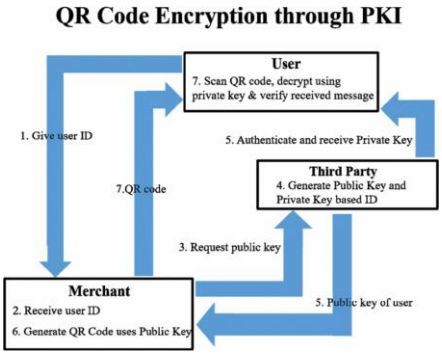

Figure 6.Structure of QR Code payment system [7]

4.2.Digital currency

Bitcoin is one of the most famous digital currencies, and it was first put forward by Satoshi Nakamoto in 2008. In the transaction of Bitcoin, a third party financial institution is not needed. This is then added to the continuous chain of hashes known as the 'Blockchain' which is a permanent record/ledger of all events witnessed on the network and can be considered the backbone of the Bitcoin network [9]. The blockchain utilizes complex mathematical algorithms to construct a chain of SHA-256 cryptographic data that cannot be replicated or altered. All transactions are added to the Blockchain and must be signed using a private key held by the owner of that particular Bitcoin which prevents third parties tampering with the transaction and Blockchain [9].

A transaction using Bitcoins requires two items; a private key and a Bitcoin address. The Bitcoin address is a random sequence of numbers and letters that makes up the Bitcoin public key and combined with a private key makes up the asymmetric key pair [9]. The sending of Bitcoins between users requires the private key of the sender for signature and the public key of the receiver. A number of confirmations are required for this transaction in order to secure the integrity of Bitcoin against tampering or hacking. The miners produce Bitcoins in the network and the blockchain ensure the safety of the trade.

5.Conclusion

This paper mainly discuss the security technology used in mobile payment system, and describes two popular MPS applications, Alipay and Bitcoin. For the users of Alipay, both security and convenience is important. And therefore, QR code technology is used in mobile app. As for the Bitcoin miners, the security requirement is even higher than Alipay users, so that blockchain is used to ensure the absolute security.

References

[1] L.You. Security Technology Analysis of Mobile Payment [J].Telecom World, 2017(06):35-37.
[2] D.Fangming. Research on Security Mechanism of Mobile Payment System [D].XiDian University, 2006.
[3] P. Chaudhury *et al.*, "ACAFP: Asymmetric key based cryptographic algorithm using four prime numbers to secure message communication. A review on RSA algorithm," *2017 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON)*, Bangkok, 2017, pp. 332-337.
[4] Junling Zhang, "A study on application of digital signature technology," *2010 International Conference on Networking and Digital Society*, Wenzhou, 2010, pp. 498-501.
[5] J. Zhu, "Study on the e-commerce security model based on PKI," *2010 International Conference on Computer Application and System Modeling (ICCASM 2010)*, Taiyuan, 2010, pp. V4-6-V4-9.

[6] S. F. Al-Janabi and A. K. Obaid, "Development of Certificate Authority services for web applications," *2012 International Conference on Future Communication Networks*, Baghdad, 2012, pp. 135-140.
[7] A. T. Purnomo, Y. S. Gondokaryono and C. Kim, "Mutual authentication in securing mobile payment system using encrypted QR code based on Public Key Infrastructure," *2016 6th International Conference on System Engineering and Technology (ICSET)*, Bandung, 2016, pp. 194-198.
[8] S. Tiwari, "An Introduction to QR Code Technology," *2016 International Conference on Information Technology (ICIT)*, Bhubaneswar, 2016, pp. 39-44.
[9] J. G. Fraser and A. Bouridane, "Have the security flaws surrounding BITCOIN effected the currency's value?," *2017 Seventh International Conference on Emerging Security Technologies (EST)*, Canterbury, 2017, pp. 50-55.