Secure Quick Response-Payment(QR-Pay) System using Mobile Device

Jaesik Lee*, Chang-Hyun Cho *, Moon-Seog Jun*

* *Dept. of Computer Science, SoongSil University, Seoul, South Korea*

j30231@ssu.ac.kr, hist0001@naver.com, mjun@ssu.ac.kr

***Abstract*— Secure QR-Pay system based on QR-code by expressing 2 dimensional can pay things between User and Shop while Offline. A shop shows payment information by expressing QR-code to display window. A user shots a situation by using mobile Device attached a camera. If a user confirms payment information and ask an approval, the payment system can be settled by itself. It's a very easy system. For this process, payment gateway(PG) helps calculate process in connection with payment. This system we proposed provides non-repudiation and confidentiality of payment information. Also, it offers mutual Authentication between user and shop to use public certificate.**

***Keywords*— Secure Payment System, QR-Code, Digital Signature, Mobile Payment, Electronic Payment**

I. INTRODUCTION

For development of IT technology, the mobile payment system using mobile payment emerges and activates in the physical payment method such as cash and credit cards[1][2]. It is the most remarkable feature that the payment system using mobile device is not paid by a physical method but by an electronic method. Also, this payment system using a mobile phone is much issued lately. Especially an efficiency of mobile phone can be used enough by comparing PC in calculation requiring counts like encryption or electronic-signification for development and rapid prevalence of smart phone. As a result the payment system in a mobile surrounding is spread with rapidity. But the payment system using an existing mobile has trouble in interacting with each affiliate or payment gateway because of adopting each different IrFM. The payment system using radio frequency signal of near field communication standards is used to solve which is having difficulty in using an existing mobile phone because the payment system carries out a role of RFID tag in mobile phone. And people have to be careful in using mobiles because of the risk in payment system such as relay attack in RFID system[3][4].

This paper transfers payment information by using an existing mobile attached a camera in QR-Code[5] and have the features that the mobile phone approves the payment by using certification and it updates softwares of the payment system in shops without additional equipment and devices. Specially, the interchange of payment information is impossible to wiretap and fulfill really attack through visible channels not wireless channels and it has characters to use electronic-signification to provide authentication and non-reputation. The composition of this study is as follows; In chapter 2 presents Secure QR-Pay system requirements and 5 phases in proposed System. Chapter 3 presents the design and implementation of proposed system. Chapter 4 presents feature analysis of the proposed system and how to prevent two types of attacks and Chapter 5 will be conclusion.

II. SECURE QR-PAY SYSTEM

Secure QR-Pay System consists of five steps. Secure QR-Pay System can register both user and shop each other through Initialization and actually payment Phase consists of four steps(***B~F step***). To use this system we proposed, a user has to get a mobile device attached a camera and available Internet. Also shop needs a Terminal that has display and communication functions. For example, a user can use a smart phone and a shop can use desktop PC connecting Internet.

A. Initialization

Both a user and shop have to issue their public certificate through public certificate authority(CA) and register theirs to payment gateway(PG) before they use Secure QR-Pay System. Each public certificate includes public key and only owners know private key that matched public key. This public key is distributed in forms of public certificate through public CA. Users install *QR-Pay client for user* in mobile terminal and also shop do. *QR-Pay client* is the system corresponding in forms of PG and Web. It gives and takes safety each by using SSL/TLS encryption protocol. Figure 1 shows initialization.

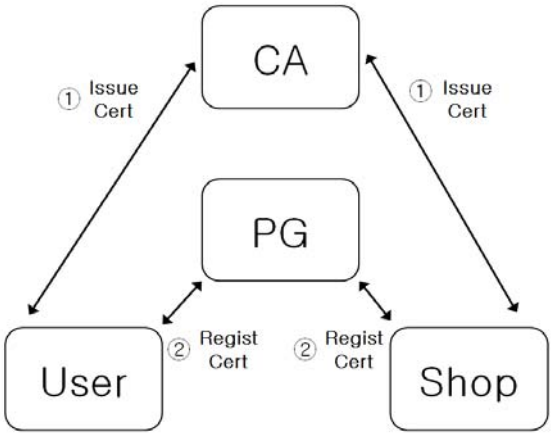

Figure 1. Initialization

B. Shop's Payment Information Creation

Shop can create pay information by using *QR-Pay Client for shop* program. Users buy goods at a shop and ask payment information and then a shop input purchase information when input of purchase information is completed. A shop do digital signature by using private key. Payment information and digital signature in value are transmitted in PG. Payment information is consists of shop number(unique numbers) to distinguish shops, unique payment numbers of each dealings issued at shop and both details of payment and the total of payment.

PG requests public certificate matching for transmitted shop numbers from public CA to verify payment Information. And PG extracts public key from shop certificate and verifies digital signature of transmitted payment information. As verification of digital signature is completed PG registers this payment information on *payment information list page* by "*Request*" and notices it at shop. This payment information can be referred by using shop number and payment number. Shop show shop number, payment number and digital signature value by QR-Code to users. Figure 2 shows payment information creation.

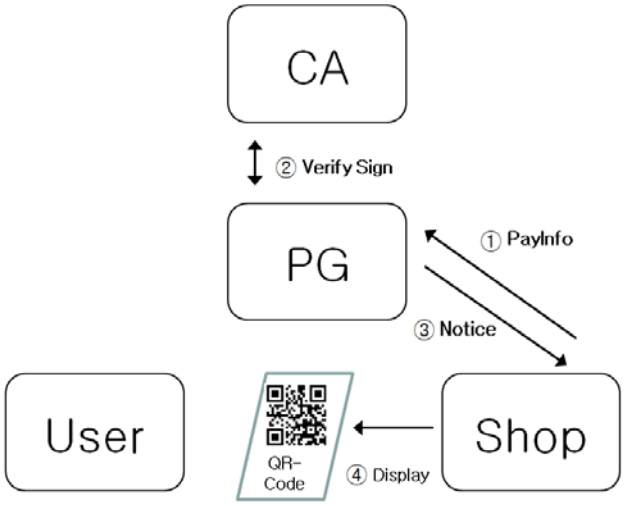

Figure 2. Payment Information Creation

C. User's Payment Information Confirmation

Users can verify payment information by using *QR-Pay client for user* program users take photographies of QR-Code by using camera of mobile device. They can find out shop number, payment number and digital signature value from this QR-code. Client programs download payment information related to payment matters on *payment information list page* of PG by using shop number and payment number. To verify transmitted payment information users request this shop's public certificate from public CA and extract shop's public key in this public certificate. By using extracted public key, digital signature can be verified. If this digital signature is verified, user's terminal shows details of payment information. Figure 3 shows payment information confirmation.

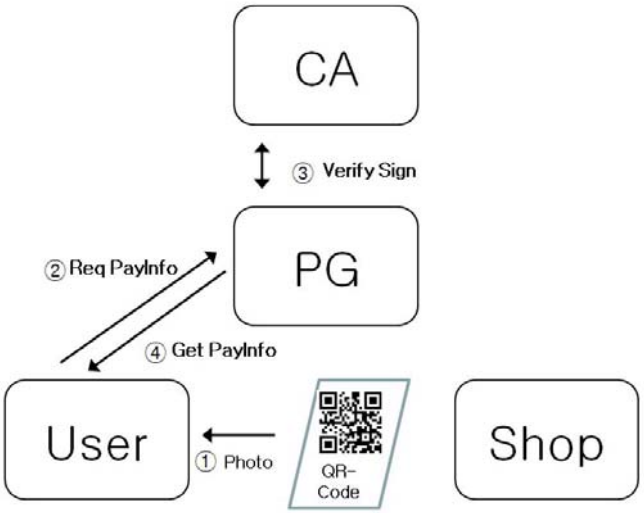

Figure 3. Payment Information Confirmation

D. User's Payment approval

Users finally check Payment Information showed to terminal at ***C step*** and details users bought. And then users approve payment. For the final payment approved, Users digital signature by using private key registered to own mobile device. Private Key is stored up to user's terminal and users input password to use private key. It is possible to access to private key as password is correct and client programs sign to paying the total about payment information by using private key. And then it transmits shop number, payment number and payment approval value to PG. Payment approval value includes paying the total. PG verify transmitted payment approval value using public certificate from public CA. Users extract public key from public certificate and then can verify it. When verify is completed PG changes '*Request*' into '*Accept*'. PG shows that payment information is changed from '*Request*' to '*Accept*' to shop. Figure 4 shows payment approval.

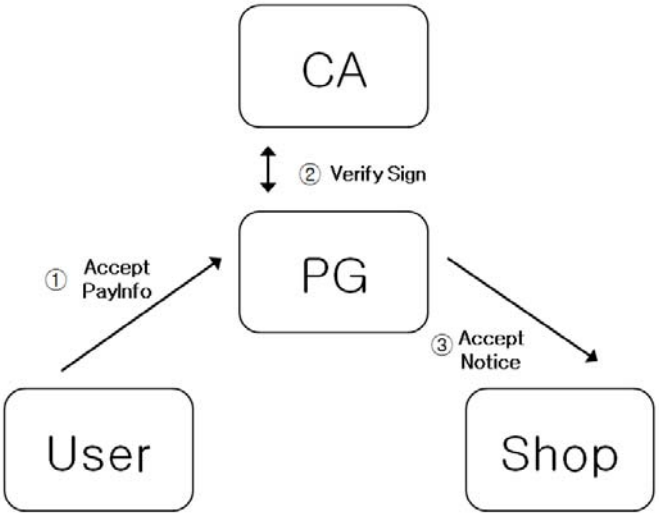

Figure 4. Payment approval

E. Payment approval confirmation

As users' payment approval is completed the reporting message completed and related to Payment Information from PG is sent to shop. In case there is nothing related to cancel or change about payment, PG changes '*Accept*' into '*Finish*' when this payment is completed. Also, Shop can delay changing approval into finish to ask payment cancel. PG reports perfectly completed approval procedures about payment information changing into "*Finish*" to shop.

III. DESIGN AND IMPLEMENTATION

In this section, we provide the design and implementation of the system implementing the proposed scheme.

A. System Design

Figure 5 shows Secure QR-Pay System architecture. The components of the system are described as followings.

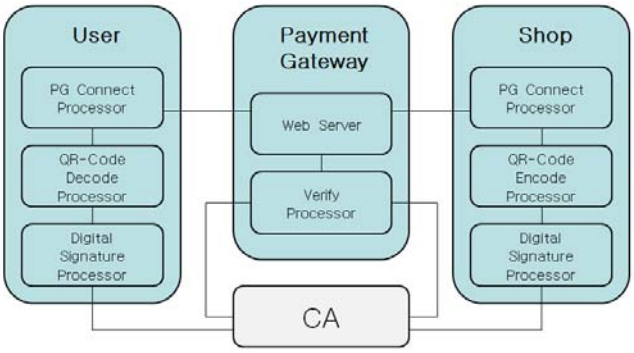

Figure 5. Secure QR-Pay System architecture

1) Payment Gateway(PG)

Web Server : It offers *payment information list page* for confirmation of users and shop to support a SSL/TLS Protocol.

Verify Processor : It verifies digital signature with getting digital signature certificate of authentication from CA for payment information verification.

2) User

PG Connect Processor : It can give and take the data by using PG and SSL/TLS Protocol safely.

QR-Code Decode Processor : It does decoding the data in value from images were taken and takes a photograph of QR-Code.

Digital Signature Processor : It verifies digital signature with a certificate of authentication. It makes digital signature regarding payment information with private key of a user.

3) Shop

PG Connect Processor : It can give and take the data by using PG and SSL/TLS Protocol safely.

QR-Code Encode Processor : It can show encoding of payment information by means of QR-Code to a monitor.

Digital Signature Processor : It verifies digital signature with a certificate of authentication. It makes digital signature regarding payment information with private key of a shop.

4) Certificate Authority(CA)

In this system use general CA.

B. Implementation

The figure 6~8 shows the implemented system screen snap shots. We use zbar code reader[6] and qrcode gen php scripts[7].

1) QR-Pay Server for PG

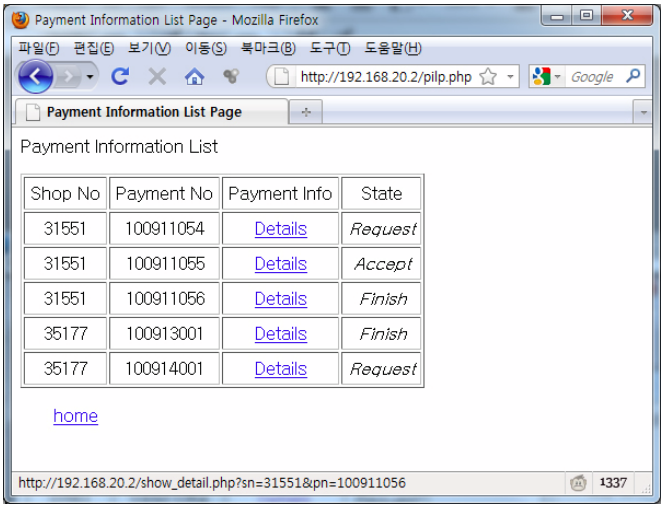

Figure 6. QR-Pay Server

2) QR-Pay Client for User

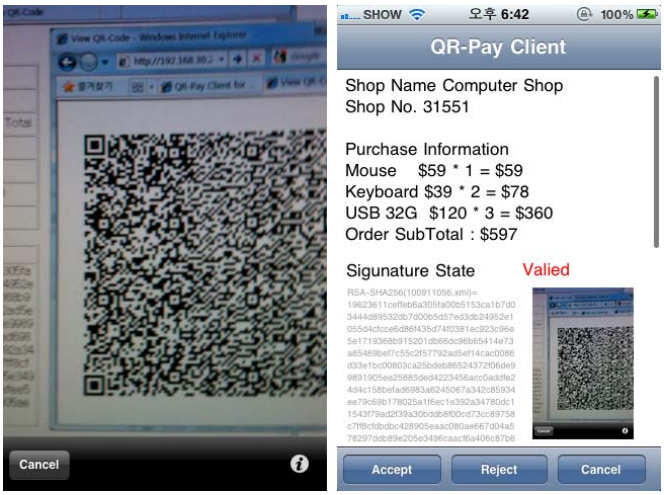

Figure 7. QR-Pay client for user

3) QR-Pay Client for Shop

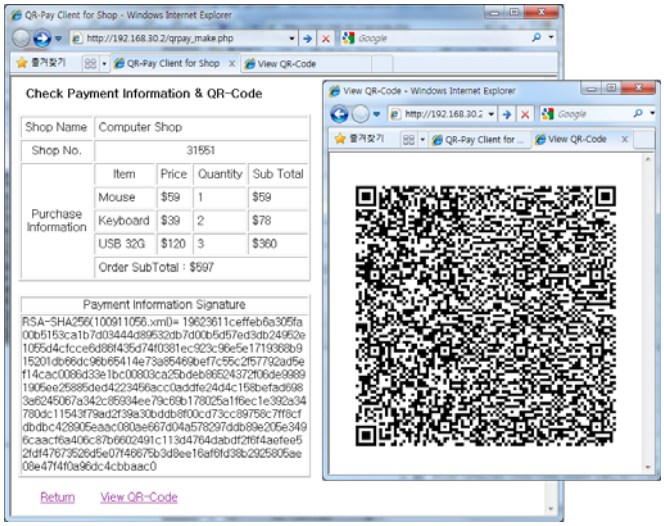

Figure 8. QR-Pay client for shop

IV. SECURITY ANALYSIS

Secure QR-Pay System provides people with mutual authentication, non-reputation, confidentiality, integrity and prevents replay attack and relay attack.

A. Mutual Authentication

Secure QR-Pay System is based on mutual authentication between a user and shop. Mutual authentication offers public certificate of public CA. That is, the shop certifies digital signature by using private key. Also, the user certifies oneself by using private key with approval of payment information. Mutual authentication is possible to get payment information through a safe channel with a middle of PG.

B. Non-reputation

Payment information does private key of the user for non-reputation. The related private key that goes with key pair and public certificate of public CA has a legal force. This method is one of the powerful non-reputation methods.

C. Confidentiality

All communication between a user and PG, PG and each shop can transmit SSL/TLS protocol through secure channel. Even if a hacker sniffe the message, he can't confirm the contents of transmitted message. Also, QR-Code transmitting visual channel can't confirm direct payment information because of only transmitting shop numbers, information numbers and digital signature in value.

D. Integrity

The shop does digital signature by using private key. A hacker can't control payment information due to nothing the private key of shop. That's why a hacker can't approve the payment. This paper we proposed provides integrity utilizing public certificate.

E. Replay Attack

All payment are granted to each unique payment number each time you pay. Transmitted payment information ever can't be done if you ask payment. In other words, it can't use replay attack that is to occur payment by using same information.

F. Relay Attack

The user and shop give and take only their QR-Code through visual channel. Even if a hacker gets QR-Code in value by attacking at glance, a hacker can't approve the payment and make QR-Code. Even so, it makes a trumped-up payment information. It is impossible to display on a monitor of this system.

V. CONCLUSION

In this paper, we proposed is the system that can pay goods more easily and simply by using mobile device. It is a very important matter to give and take payment information related payment through secure channel. For solving this matter, proposed system is not directly transmitted payment information but QR-Code by expressing 2 dimensional that has a constitution to get digital signature in value. It can be a safe structure due to confirmation directly compared with available wire tapping channel such as a wireless channel. Also, proposed system offers mutual authentication, non-reputation, confidentiality, integrity using public certificate of public CA. Finally, proposed system prevents replay attack and relay attack.

ACKNOWLEDGMENT

This work was supported by the SoongSil University Research Fund.

REFERENCES

[1] H. C. Cheng, J. W. Chen, T. Y. Chi and P.H. Chen, "A generic model for NFC-based mobile commerce", in Proc. ICACT'09, 2009, pp.2009-2014.

[2] Michael Silbermann, "Security Analysis of Contactless Payment Systems in Practice", Diplomarbeit, Ruhr-Universität-Bochum, November 2009.

[3] J. H. Kim and H. W. Kim, "Security Vulnerability and Considerations in Mobile RFID environment," in Proc. ICACT'06, 2006, pp. 801-804.

[4] Ziv Kfir and Avishai Wool, "Picking Virtual Pockets using Relay Attacks on Contactless Smartcard", in Proc. SECURECOMM'05, 2005, pp.47-58.

[5] (2010) The QR-Code Site. Available: http://www.denso-wave.com/qrcode/index-e.html

[6] (2010) Zbar Code Reader. Available: http://sourceforge.net/projects/zbar/

[7] (2010) QRcode PHP scripts ver 0.50 Available : http://www.swetake.com/qr/qr_cgi_e.html