Research on Quickpass Payment Terminal Application System Based on dynamic QR Code

Hu Baidong¹, Zhou Yukun²

¹ Hangzhou Sunyard Technology Co. Ltd, Hangzhou 310053, China;
² Zhejiang Business College Applied Engineering College, Hangzhou 310053, China
E-mail: 12853962@qq.com

Abstract: A dynamic QR code quickpass terminal application system is designed in this paper, the system is a convenient receiving application system for QR code scanning and being scanned, the dynamic QR code (each bill a single code) can be generated and displayed based on the network and the real-time order information, replacing the commonly used forged static QR code patches, so as to improve the previous payment security environment and greatly reduce unnecessary losses for merchants and operators.

1. Introduction
Small and medium-sized operators in the market have long adopted a large number of stickers or cards in the form of static QR code collection or transfer mode, the static QR code sticker in its collection or transfer mode is often easy to be caught by illegal person in management, stealing the business proceeds of a merchant by replacing or covering the original merchant code with minimal forgery and low cost, this method is concealed, difficult to be discovered by small and micro operators in time, and because of its low cost of forgery, it is easy to be repeatedly used by illegal person. QR code payment technology has become one of the main payment methods of O2O in the mobile Internet era. Its simple, fast and low-cost characteristics make it widely used in small and medium-sized micro-merchants.

"Quickpass payment" is an innovative payment method based on master card simulation and token technology introduced by China UnionPay. It directly simulates a quickpass payment card of an entity bank card in a bank client, and supports handsets with near-field payment function to pay by contactless POS entity stores and the Internet. In order to solve the problem of QR code forgery and respond to the convenient payment strategy of UnionPay, the quickpass payment terminal developed in this paper can complete QR code transaction, UnionPay transaction and dynamic QR code generation and display by using Wi-Fi or GPRS to access the backstage through the internet.

2. QR code technology

2.1 Present situation
QR code has become one of the important media in the mobile marketing era, which combines interactive marketing with precision marketing, and gradually shows its value-added role because of its many characteristics and advantages, such as large amount of information, strong convenience, low production cost, low entry threshold and high economic efficiency. According to the latest data released by the Analysis, in the first quarter of 2017, China's third-party payment mobile market
transactions amounted to 18809.12 billion CNY, an increase of 46.78%. According to analysis, by 2019, the China Mobile payment market will reach 100 billion CNY. The rapid expansion of the market has promoted the continuous innovation of technology, and has also given rise to a variety of payment methods. QR code payment stands out for its convenient operation, the efficiency of receipt and the property of moving. It has become a weapon for all trades to compete for the entrance of traffic. At present, QR code has been widely used in mobile communications, cultural performances, transportation, finance, catering, entertainment, tourism and other industries, including electronic ticketing and vouchers, enterprise daily marketing, convenient life and so on[1].

2.2 Overview of dynamic QR code
A QR code is a geometric object that uses several corresponding binary graphics to represent recorded data information on a plane. As an advanced application, with the popularization of mobile Internet and intelligent terminal, it has been rapidly popularized in many fields and served as a bridge for data transmission. QR bar code has the advantages of large information capacity, high density, strong error correcting ability, good security and wide encoding range. It can also introduce check and correction code, and has the ability to detect errors and recover deletion errors[1-2]. In traditional QR code, the reuse of static data increases the risk of loss, leakage and cracking, and reduces the security factor of information system. Dynamic QR code is based on the traditional QR code in a period of time multi-frame QR code image alternate display, each frame of QR code image data are generated by different key dynamic encryption, not easy to forge and not easy to crack. Each frame of QR code has timeliness, which can better ensure the safety of data, dynamic QR code generated by special equipment, short period of validity, basically one code at a time, so it is high security[3].

2.3 QR code and mobile terminal
The functional development of mobile terminals is the driving force to promote the development of QR code mobile marketing business, therefore, the design and development of mobile terminal equipment must be combined with changes in consumer demand, through the two-way upgrading of mobile terminal hardware and software, to strengthen the ability of mobile terminal data processing and conversion. In the aspect of technology development, the most important thing is to further enhance the security of QR code, obtain the required information by scanning QR code under the condition of guaranteeing the privacy of customers, strengthen the identification function of QR code technology, and resist malicious attacks such as mobile phone viruses, phishing websites. QR code payment can be divided into two categories: cardholder scanning merchant QR code and merchant scanning cardholder payment QR code, the dynamic QR code is generated by special equipment, the validity period is short, basically one time one yard, and the security is high.

3. Terminal system architecture

3.1 System internal schematic diagram
The internal schematic diagram is shown in Figure 1, including K21 security processor, LCD dynamic QR code display, 7-segment digital display, interface power supply, WI-FI, GPRS wireless communication, contactless circuit, voice broadcast and keyboard input modules.
3.2 Hardware block diagram
The quickpass terminal application system downloads the application by USB-CDC, and the communication port is Micro USB. The hardware block diagram, like Figure 2 below, is divided into three parts: power module, communication module and working module[4].

- Power module: provided by the communication interface USB.
- Communication module: USB communication, WIFI communication (optional), GPRS communication (optional), which WIFI and GPRS in one of the two options.
- Working modules: contactless module, LCD, keyboard, Out-of-chip SPI Flash (4MB), module for preventing disassembly, RTC (power is supplied by button batteries when power is out), six-digit digital tube, contactless LED lights, audio module, scanning head (optional).

3.3 Software system
The software system block diagram of terminal module is shown in Figure 3. The program is divided into three layers: ISP layer, API layer, application layer. The ISP layer is the abstract layer of the operating code for hardware devices, and provides a unified interface for the API layer to improve the portability of the code. API layer is the abstract layer of common function and driver code, providing a unified interface for application layer, and facilitating the development and transplantation of application layer programs. The application layer, also known as the APP layer, is the code layer for the specific implementation of the business.
3.4 QR code payment system architecture
The dynamic QR code payment architecture is shown in Figure 4. QR code processing system is completed by QR code display, collection and payment, etc.

4. Dynamic QR code generation and encryption and decryption process

4.1 Asymmetric key management
Quickpass payment terminal networking achieve QR code scanning and being scanned transactions, online dynamic QR code generation equipment must be equipped with SE security unit for storage and protection of asymmetric key information, with self-destruction function[5]. The asymmetric key algorithm signature mechanism is used to ensure the security of the communication message between the on-line dynamic QR code generator and the background system. The asymmetric key is stored in the security unit (SE). When the terminal generates the on-line dynamic QR code, the symmetric key is used to compute the Mac with the communication message of the background system. The symmetric key of the POS machine is stored in the POS security unit. A dynamic QR code can only be used for one-time scanning payment.

4.1.1 Merchants network access. Acquirers apply to the UnionPay network access for merchants. UnionPay distributes merchant information, UnionPay public key and merchant private key certificate download address to acquirers. Acquirers or merchant download the relevant certificate according to "two codes and user name of merchant distribution certificate" in CFCA, and upload the merchant public key to the UnionPay merchant service platform, and the private key is filled into the offline equipment, which is used for the offline dynamic collection code signature.

4.1.2 Key generation and transmission. On-line dynamic QR code generation equipment should support the generation of public and private key pairs, private key exists in the security SE unit, which
is not allowed to be derived in any way, public key can be derived, and submitted to the receiving unit with equipment unique number. Related key generation, transmission, filling and deletion must comply with relevant industry and UnionPay enterprise standards[6], and use the asymmetric algorithm SM2 private key to make a signature for the digest.

4.2 Encryption and decryption scheme

4.2.1 Algorithm. Secret key is generated according to SM4's key algorithm in this project. SM4 block cipher algorithm is a symmetric block cipher algorithm designed by our country. It is used to encrypt and decrypt data to ensure the confidentiality of data and information. The basic condition for ensuring the security of a symmetric cipher algorithm is that it has enough key length. The SM4 algorithm has the same key length as the AES algorithm, and the packet length is 128 bits. Therefore, the security is higher than the 3DES algorithm[7].

4.2.2 Process. The encryption device first generates the key according to the SM4 key algorithm, and then records the key to the database in the backstage. The operator exports the key to the management platform, and imports it into the device, then pours it into the terminal. During the transaction, the terminal encrypts the message data with the key. After receiving the message in the backstage, it calls the encryption device interface and transmits the data to the encryption device. Encryption device returns the result of decryption, and then backstage processes the business logic[8].

5. System function

5.1 QR code correlation function
typedef struct{
    unsigned char *src_data;
    int src_len;
    unsigned char* enc_buf;
    int enc_len;
    int width;
    int rowsize;
}QR_Code_t;
typedef struct{
    unsigned int x;
    unsigned int y;
    unsigned int magnification;
}QR_Code_DispConfig_t;

5.2 Encryption algorithm function

5.2.1 SM2 encryption algorithm.
//SM2
typedef struct
{
    unsigned int nAlgID;
    unsigned int nBits;
    unsigned char X[32];
    unsigned char Y[32];
} SM2_PubKey;

//SM2
typedef struct
{
    unsigned char pKey[32];
} SM2_PrivateKey;

5.2.2 SM4 encryption algorithm.

Table 1. PubCrypt_SM4 function.

| Function name | PubCrypt_SM4 |
|---------------|--------------|
| Function prototype | int PubCrypt_SM4(char *dst, char *src, int length, char *key, char flag) |
| Function description | SM4 ECB |
| input parameter | src(in) |
| | length(in) |
| | key(in) |
| | flag(in) |
| | 'E', 'e' |
| Output parameters | dst(out) |
| | RETURN SUCC |
| | RETURN_FAIL |
| Return value | N/A |
| Is there function preprocessing | N/A |
| Functions invoked in function implementation | N/A |

6. System circuit board
The system circuit board is shown in Figure 5, PCB is a four-layer board, the circuit board material is FR4, the surface is deposited with gold, the thickness of the board is 1.6 mm, the area is 130 * 69 (mm).

![Figure 5. System chip layout.](image)

7. Test result
The test results of QR code scanning mode are shown in Figure 6. The merchant terminal generates dynamic QR code, the amount is CNY 0.01. The cardholder pays by scanning QR code scanned in APP. The payment is successful. The merchant terminal shows that the transaction is successful and the transaction is completed.
The test results of QR code being scanned mode are shown in Figure 7. The cardholder APP generates QR code for payment, and the merchant terminal scans QR code generated by the pier. The amount is CNY 0.01. The payment is successful. Both the customer APP and the merchant terminal show that the payment is successful and the transaction is completed.

8. Conclusion
A quickpass payment terminal application system based on dynamic QR code is designed in this paper. The dynamic QR code (each bill a single code) can be generated and displayed through the network according to the merchants and real-time order information, replacing the static QR code pester which is easily forged by the original shops, thus improving the original payment security environment, greatly reducing the unnecessary losses of merchants and operators. Practical application and test results show that the system can generate and display QR code information, and have the payment function by both scanning and being scanned, which greatly improves the security performance of payment system.

Acknowledgments
Thank the project team members for their support and contribution.

References
[1] Zhou Hong, Xiao Qianhui. (2014) Application analysis of QR code in mobile marketing. Commercial Times, 17: 85-86.
[2] PAVLIDIS T, SWARTZ J, WANG Y P. (1992) Information encoding with QR bar codes. IEEE Computer, 25(6): 20-28.
[3] Guo Quanzhong. (2014) The status and future of QR code. News and Writing, 7: 22-25.
[4] Xu Ling, Jiang Xinzhi, Zhang Jie. (2012) Design and implementation of QR code recognition system in mobile phone. 32-5:1474-1476.
[5] China Commodity coding Center, (2003) Bar Code Technology and Application. Tsinghua university press, Beijing.

[6] Ma Lilin. (2016) An identity authentication scheme of mobile terminal based on QR code in cloudcomputing environment. Microelectronics and computer, 33: 34-39.

[7] Gui Zhenwen, Wang Yongtian, Liu Yue, Chen Jing. (2014) Study on the application of QR code in mobile augmented reality. Journal of computer-aided design & computer graphics. 26: 34-39.

[8] China UnionPay QR code payment security specification (Q/CUP 067-2016).