A Survey of Technologies for Mobile Payment Security

Wenzheng Liu, *Student, NUDT,* John Doe, *Fellow, OSA,* and Jane Doe, *Life Fellow, IEEE*

***Abstract*—Nowadays, the rising penetration of smartphones and the important roles of them in peoples daily life make the smartphones an ideal medium to conduct payment transactions. The smartphones are capable to store everything that would normally be carried in a physical wallet and also allows the users to make payments anytime and anywhere. The potential added-values of mobile payments, such as generating new revenues, obtaining new users, increasing user stickiness attracted different players to expand their businesses to the mobile payment services, including financial institutions, mobile network operators, mobile device manufacturers, trusted third party providers. To compete in the market, they explored different technologies and business models which resulted in the complexity and dynamics of the mobile payment market. Consequently, mobile payments have only become a standard practice in a few countries. In terms of proximity payments, NFC is widely viewed as one of the most promising technologies due to its security features, compatibility with the existing financial infrastructures, and ease of use. In the Chinese market, compared with QR code, NFC was first introduced and supported by various players. However, the Chinese mobile proximity payment market has become the largest and fastest-growing mobile proximity payment market in the world in few years by utilising QR code. The market is highly concentrated with Alipay and Tenpay which are QR code-based mobile payment platforms. In other words, QR code overtook NFC and became the most popular mobile proximity payment technology in China.**

***Index Terms*—token, payment, offline, LATEX, online, TOTP.**

I. Introduction

IN this study, the research model is developed based on relevant business model, platform and business ecosystem theories. The final research model consists of three connected perspectives Chinese mobile payment platforms, namely, He Wallet, Alipay and QuickPass which have implemented one or several technological solutions based on NFC and QR code technologies. The data for the case studies is collected from the semi-structured interviews and the desk research. The results showed that although NFC technology was adopted first in the Chinese market, the enabling devices of both consumers and merchants were not widely ready at that time for NFC technology,but good enough for QR code technology. However, the early NFC adopters (both MNOs and financial institutions) were reluctant to make a huge investment in the enabling devices to realise the large-scale deployment in the early stage due to the uncertainties on the technology level and the unclear roles and benefits on the business aspect. Thereby, they missed the best time to capture user and develop users' habit. In contrast, Alipay strategically adopted the independent service provider mode to leverage its obtained platform resources and capabilities which significantly contributed the mass adoption of QR code in the Chinese market. Despite QR code currently dominated the Chinese mobile payment market, it is believed that NFC has its place in the Chinese mobile payment market as China UnionPay adopted an open platform strategy to incorporate all relevant players into its ecosystem to facilitate the development of NFC-based mobile payments.

M. Shell was with the Department of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA, 30332 USA e-mail: (see http://www.michaelshell.org/contact.html).

J. Doe and J. Doe are with Anonymous University.

Manuscript received April 19, 2005; revised August 26, 2015.

A. Subsection Heading Here

Subsection text here.

1) Subsubsection Heading Here: Subsubsection text here.

II. Virtual Bank card binding technology

Virtual bank card instead of the real bank card binding in the payment account or mobile terminal and transfer in the transaction.In this section,the Virtual bank card binding technology will be told. First, It is need to know why the virtual bank card need bindind in the mobile phone.Accoding to the PCI DSS and China UnionPay standard,there three main reasons need to explain. First,If the magnetic stripe card is skipped, it can be easily copied into a fake card, which is used for fraudulent transactions and brings about capital losses to the cardholder.in addition,If the card number is expired and the validity period, it is easy to move in some e-commerce in fraudulent transactions, bringing the cardholder money losses.moreover,In the online payment and mobile payment environment,the card organization is even more hopeful that it will not change the usage habit of the cardholder completing the transaction with the card number and expiration date, and at the same time effectively improve the payment security.

A. The process of binding bank card.

The payment provider hands over the bank card account (PAN) which the user needs to bind to the corresponding bank server. If the corresponding virtual bank card for this PAN does not exist for this merchant in the public central database,a new virtual is generated and an entry is added to the public central database.At the same time return virtual bank card to the merchant. The merchant binds the token with the user's account as a virtual bank card corresponding to the PAN.

However, in order to prevent the payment provider to saving or leaking the user's real bank card information, Alipay has proposed a new virtual bank card binding scheme:

1, the merchant system pre-save the payment system server authorization certificate. And authorize the signature of the authorization certificate called its default instructions.

2. The merchant system receives a binding request sent by a terminal, where the binding request corresponds to a user account that the user logs in on the merchant system; and returns a preset instruction to the terminal;

3, the terminal to the payment system through the secure channel to send the default instructions and the real bank card number.

4, the payment system generates a virtual bank card number corresponding to the real bank card number. (For each real bank card number generated by the virtual card number is different)

5, the virtual bank card number returned to the terminal.

6, the terminal sends the virtual bank card number to the payment provider.

7, the payment provider bind the virtual bank card to the user accounts.

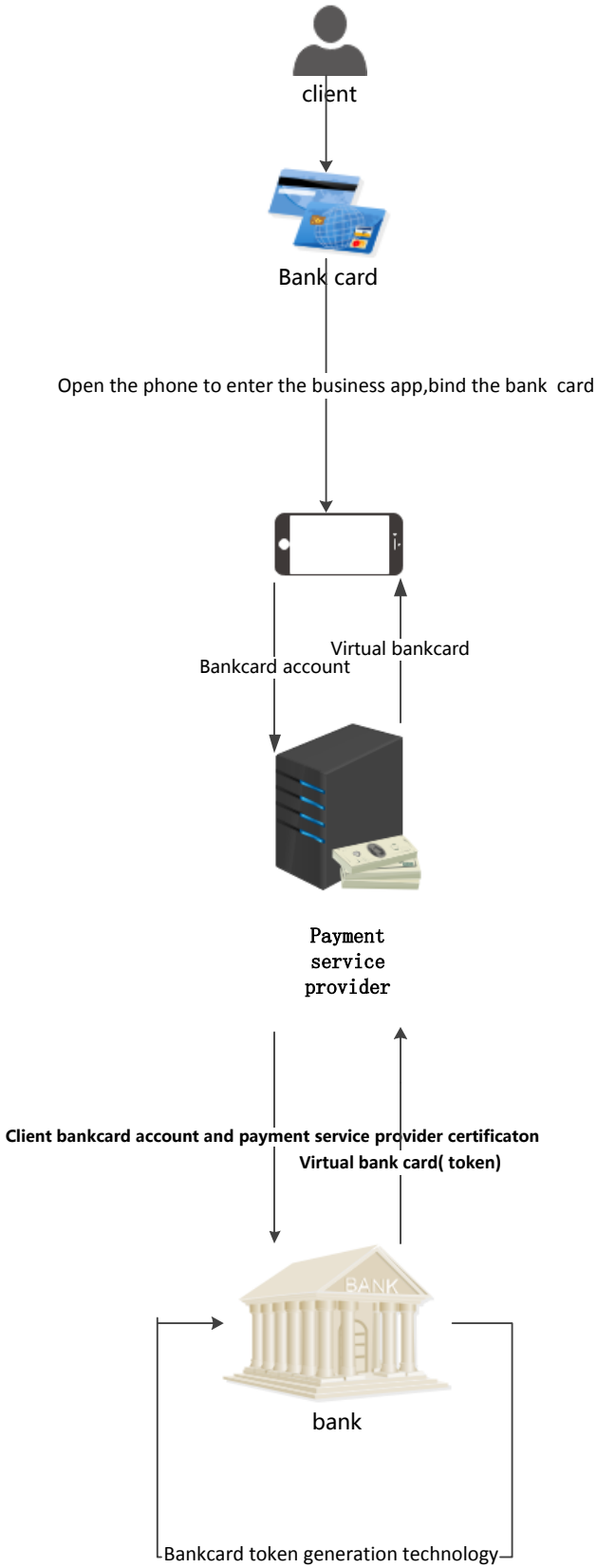
In this scheme, the payment provider can not get the user's real bank card account information.

B. Fundamental of virtual bank card: payment tokenization

In our digital age, bank cards have become a popular payment tool. With the increasing popularity of business through the Internet, each company needs to maintain its customers' bank card information in some form. The theft of bank card data is considered to be one of the most serious threats to any company. Such violations will not only bring serious economic losses to the company, but also cause serious damage to the brand image.

The Payment Card Industry Security Standards Council (PCI SSC) was established by a major payment card company and is an organization responsible for the best development and deployment.The organization that ensures the security of credit card data. In particular, PCI SSC has developed a standard PCI Data Security Standard (PCI DSS) called "Standards" [11], which specifies the security mechanism card data required to guarantee payment. PCI DSS requires organizations that process card payments to protect cardholder data as they store, transmit, and process them. The practical requirements specified by the PCI DSS are very detailed and complicated. In order to achieve PCI compliance, merchants need to provide security policies regarding the use and use of the document regarding all sensitive information stored in their environment. Considering PCI compliance requires the confidence of its customers for any business. In addition, in some countries, a company that is exposed to theft of sensitive information may face a large amount of fines.

Enterprises, merchants, and payment processors face severe, ongoing challenges securing their networks and high-value sensitive data such as payment cardholder data, to comply with the Payment Card Industry Data Security Standard (PCI DSS) and data privacy laws. Tokenization, which is used as a way of replacing sensitive data like credit card numbers with tokens, is one of the data protection and audit scope reduction methods recommended by the PCI DSS.



The principle is to verify the transaction by using a payment token instead of a real bank card number so as to prevent card number information leakage risk. Payment tokenization is the process of replacing a traditional bank card master account with a unique numeric value, while ensuring that the value's application is limited to a specific merchant, channel, or device. Payment tags can be used in all aspects of bank card transactions, and existing bank card number based on the same transaction, can be used across industries in the industry, has versatility. As the latest cutting-edge technology in the global payment field, payment tokenization technology has its advantages in three aspects:

First, there is no need to retain sensitive information, cardholder card number and the validity of the card does not appear in the transaction;

Second, payment tags can only be used in a limited transaction scenario, making payments more secure;

Thirdly, compared with the traditional bank card verification function, the payment tag integrates the functions of personal identification and device information verification, additional verification of payment information and risk rating to conduct transaction legitimacy identification and risk control. Therefore, the tokenization of the payment can not only prevent the leakage of sensitive information of cardholders in all aspects of transaction, but also reduce the probability of fraudulent transactions.

The international chip card standardization organization EMVCo has defined smart card payment and also defined a token (ie token) as a substitute in the actual card application. Merchants can handle cards and tokens in the same way, which means that there is no need to change the already installed and installed PoS (Point of Sale) terminals. This clever processing is done through a Token Service Provider (TSP) that has the actual card information. When issuing token Tokens, you can flexibly make some restrictions, such as the use of only certain businesses, online use only, offline use, and you can limit the value, time and location of tokens, such as The security level of the device determines its effective time. When necessary, tokens can be destroyed and re-issued. The Tokens solution ensures compatibility with existing infrastructure and saves money. Working with HCE, the token can solve the problem of availability. When the mobile network is unstable, the token is stored locally on the mobile phone and can be paid offline. The EMVCo Payment Token Specification Technical Framework v1.0 provides examples of secure storage of tokens on a device. For example, it can be stored in a trusted execution environment TEE. In addition, tokens can be used through any channel, such as NFC HCE, Internet transactions, and Bluetooth Beacons, so the technology is not limited to PoS terminals.

As described in [10], a tokenization system has the following components:

1.A method for token generation A process to create a token corresponding to a primary account number (PAN). Some of the mentioned options are encryption functions, cryptographic hash functions andrandom number generators.

2.A token mapping procedure It refers to the method used to associate a token with a PAN. Given a token, this method

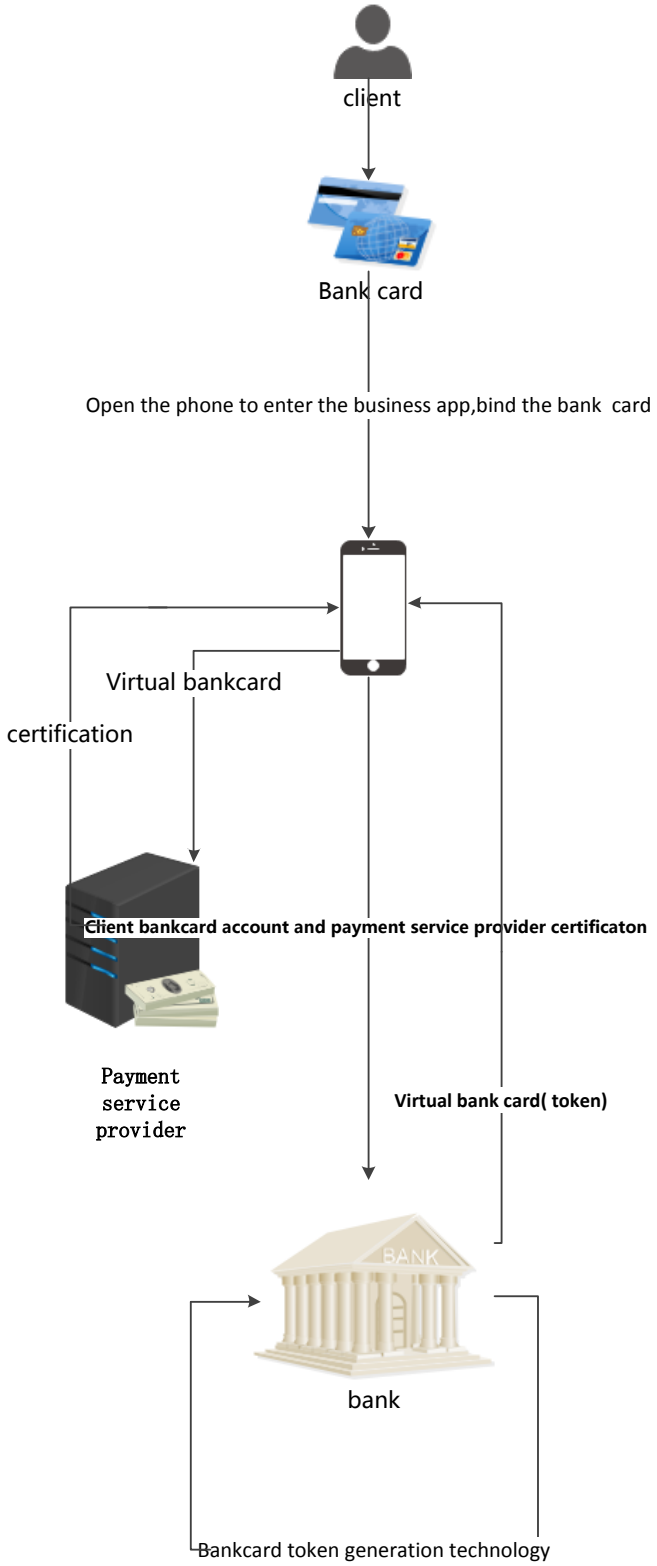


Fig. 2. Token application process.

will allow the system to recover PAN.

3.Card-Vault It is a repository that typically stores pairs of PANs and tokens and other information needed for token mapping. Since it may contain PAN, it must be specially protected according to PCI DSS requirements.

4.Cryptographic Key Management This module is a set of mechanisms for creating, using, managing, storing, and protecting keys used to protect PAN data and data involved in token generation.

It is two basic requirements for tokens and tokenization systems.

Format Preserving The token should have the same format as the PAN so that the stored PAN can be easily replaced by the token in the merchant's environment. In addition, it is important to distinguish the token from the PAN token easily.

Uniqueness The token generation method should be deterministic. The tokens for a specific PAN should be unique,In a specific payment environment two different PANs should be represented by different tokens.

Article [10] discusses the security of tokenization systems.the author consider three different attack scenarios:

1. IND-TKR : Tokens are only public. This represents the most realistic scenario where an adversary has access to the tokens only, and the card-vault data remains in-accessible.

IND-TKR refers to the basic security requirement for tokens. It adheres to the informal security notion for tokens as stated in the PCI DSS guideline for tokenization. It models the fact that tokens and PANs are un-linkable in a computational sense, if the key and card-vault are kept secret. Thus, if a merchant adopts a tokenization scheme provided by a third party, which is secure in the IND-TKR sense then this will probably relieve it from PCI compliance. As in this case the merchant does not own the card-vault or the keys, and the burden of security involved with the keys and the card-vault lies with the provider who offers the tokenization service.

2. IND-TKR-CV : The tokens and the contents of the card-vault are public. This represents an extreme scenario where the adversary gets access to the card-vault data also.

The IND-TKR-CV is a stronger notion. If a tokenization system achieves this security, then it implies that tokens and PANs are un-linkable even with the knowledge of the card-vault. This in turn implies that the contents of the card-vault are not useful (in a computational sense) to derive a relation between PANs and tokens. Thus, it provides security both to the tokenization service provider and the merchant who use this service.

3. IND-TKR-KEY : This represents another extreme scenario where the tokens and the keys are public.

IND-TKR-KEY is a stronger form of the IND-TKR notion. Some public documents like [17] it has been stressed that encryption is not a good option for tokenization, as in theory there exists the possibility that a token can be inverted to obtain the PAN. If tokens are generated using a secure encryption scheme, then it is infeasible for any reasonably efficient adversary to invert the token without the knowledge of the key. But, this computational guarantee does not seem to be enough for users. The IND- TKR-KEY definition aims to model this paranoid situation, where linking the PANs with tokens becomes infeasible even with the knowledge of the key. Note in IND-TKR-KEY we still assume that the card-vault is inaccessible to an adversary.

All the definitions follow the style of a chosen plaintext attack. The definitions may be made stronger by giving the adversary additional power of obtaining PANs corresponding to tokens of its choice. But in this application, we think such stronger notions are not applicable.

the [10] also give the security proof of Tokenization Using FPE and Tokenization Without Using FPE.For details, please check the the article

Tokens and tokenization solutions can be implemented in numerous ways, and the security or process controls provided by one solution may not be suitable or applicable to another. Additionally, the assignment of roles and responsibilities may vary according to the particular solution or deployment method, and all entities involved should be aware of their obligations for maintaining security controls and protecting cardholder data.[10]

The level of PCI DSS scope reduction offered by a tokenization solution will also need to be carefully evaluated for each implementation. For example, locations and flows of cardholder data, adequacy of segmentation, and controls around de-tokenization and mapping processes should be reviewed and verified to ensure proper scoping of the CDE and appropriate application of PCI DSS security requirements.[10]

1) Centralized tokenization technologies: Centralized tokenization is conventional, database-centric solutionswhich requst the token corresponding to the provided PAN from a common central database. If no token corresponding token exists in the common central database at the time of the request, a new token is generated and an entry will be added to the common central database.

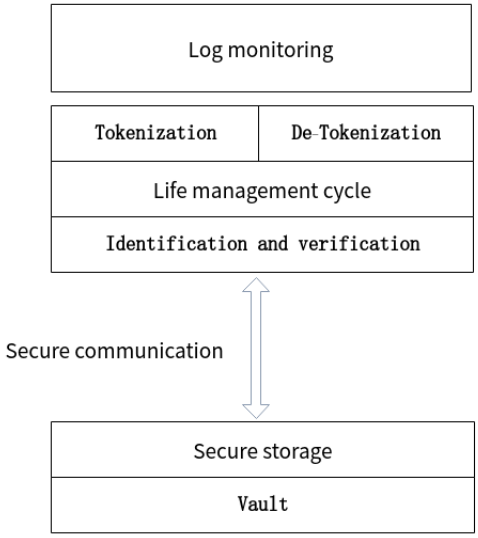


Fig. 3. token service provider

Card organizations are highly recommended centralized

tokenization technologies. Centralized tokenization involves building a large-scale database (token vault), storing each PAN together with a generated token. Figure 3 shows the China UnionPay payment tokenization system framework

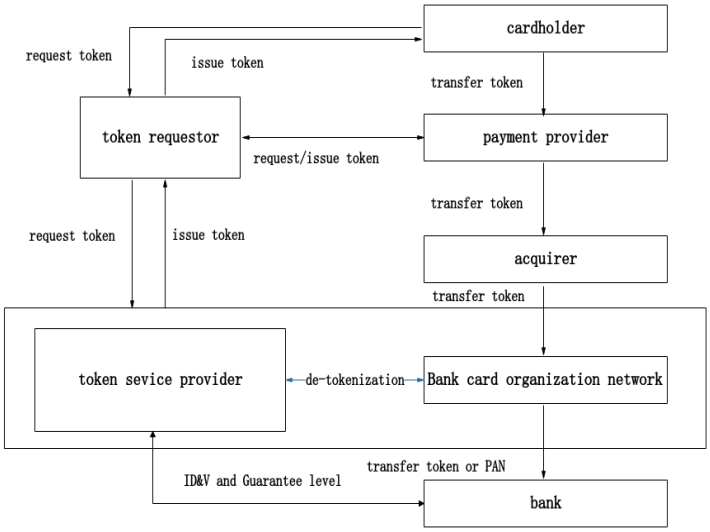


Fig. 4. China UnionPay payment tokenization system framework

2) Distributed tokenization technologies:

III. Communication method

Mobile payment communication is mainly used for short-distance communication, especially for poor mobile network environment offline payment. Payment information is delivered via these means of communication. Many people regard communication as a means of payment. However, they are only responsible for transmitting payment information. The real means of influencing payment are payment encryption and authentication technologies.

A. QR code

QR code was invented in 1994 by Denso Wave, a Toyota subsidiary of Japan. The QR code not only has large information capacity, high reliability, and low cost, but also can represent various character information such as Chinese characters and images, and has strong security against fraud and is very convenient to use. Therefore, it quickly became popular in Japan and South Korea. Since then, European and American countries have begun to use it in large quantities.

QR code payment is very popular in China, people can almost go out without wallets and bank cards. You only need to show the QR code on your mobile phone to be able to pay in most places even without network. However, why is it possible to authorize payment with the QR code?

However, the QR code itself cannot make payment authorization, since the actual payment authorization is the payment certificate which encoded in the QR code. The payment certificate is a series of digits(which we calld **payment password**). You can authorize payment with this numbers. So the role of the QR code in mobile payment is to transmit this series of numbers. The specific technology of payment certificate will be told in section 4.

In this subsection, the QR code technology will be introduce.

The QR code is one of the two-dimensional code, which is similar to the magnetic stripe. The magnetic stripe transforms the information into a track through a certain law, and the two-dimensional code transforms the information into a graph. Reading the magnetic stripe reads the track through the reader and then converts back to the original information, while the two-dimensional code reads the graphics through the camera and then converts back to the original information.

Stacked two dimensional bar code: It consists of multiple rows of bar codes stacked together. Its shape is similar to that of one-dimensional codes. The encoding principle is similar to the encoding principle of the same dimension codes. It has the same or similar characteristics as the one-dimensional bar code in terms of coding design, reading mode, and verification principle, and can even be read and scanned with the same device, except that the reading and decoding algorithms are different from the one-dimensional bar code. Larger capacity but usually does not have error correction. Representatives are:

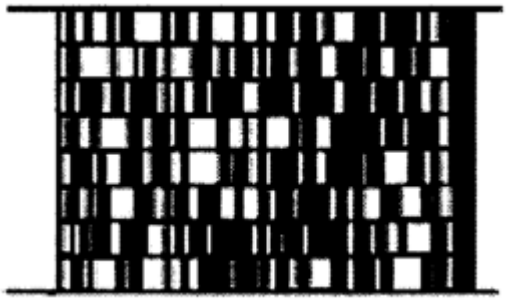


Fig. 5. code 49

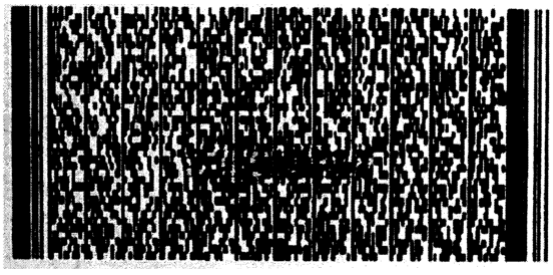


Fig. 6. PDF 417

Matrix type two-dimensional bar code: A matrix consisting of dark squares and light squares, usually square, where the dark and light blocks represent 1 and 0 in binary, respectively. Matrix-based two-dimensional code is a graphical symbol automatic identification and processing code system, which usually has error correction function. Typical examples are DM codes, QR codes, and Hanson codes.

The QR code has a total of 4 error correction levels, represented by L, M, Q, and H, respectively, and the recoverable code word ratios are 7%, 15%, 25%, and 30% in

order. The higher the error correction level used is, the more error correction code words are used, and the fewer code words are used for encoding information. (In which the related technology mainly uses error correction code)

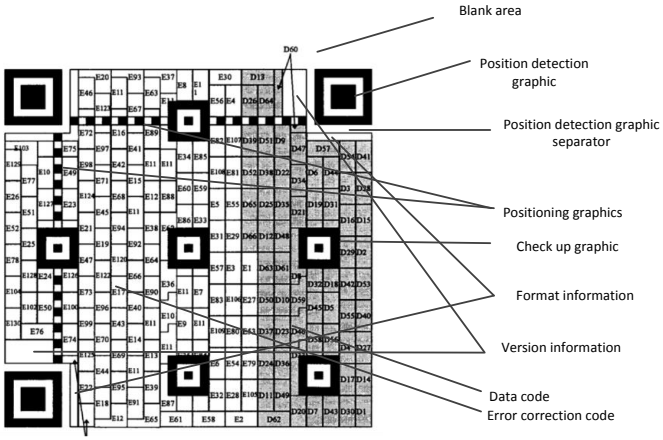


Fig. 7. The structure of the QR code

The Fig 7 shows the structure of the QR code:

Check up graphic: The Check up graphic looks similar to the position detection pattern, but the middle square has only one unit. It is mainly used for the correction of the QR code, especially the correction of the graphic distortion caused by the different camera angles or the uneven surface of the printed object. Depending on the version, the number of correction patterns is not the same. There is no correction pattern for version 1 and version 40 contains 46. Wechat's payment code belongs to version 1 so there is no correction graphics, and Alipay's payment code belongs to version 2, there is one.

positioning graphic The positioning graphic is two alternating dark and light bands, and the table is defined on the two-dimensional code like a ruler.

Format and Version information: The format information and version information record the format and version of this QR code and have their own separate calculation rules.

Data and Error Correction code: After the error correction coding of the data is completed, the final code word sequence is constructed in a certain order for the data code word and the error correction code word. The low code word of each data block is in front of the sequence, and the data code word is arranged in front of the error correction code. According to the first codeword of data block 1, the first codeword of data block 2, ..., the last codeword of data block n; the first codeword of error correction code 1, error correction The second codeword of code 2, ..., the last codeword of error correction code n

B. NFC

Near field communication (NFC) is a wireless technology operating in the short range of four to ten centimeters for communication. It is based on radio frequency identification (RFID) technology. For a communication, an NFC device generates a radio frequency in 13.56 MHz spectrum. A receiver could receive the data through the principle of magnetic inductive coupling if it lies in a close proximity. Transmitter and receiver are small chipsets which are able to be embedded in devices such as mobile phones, POS (Point Of Sale) terminals, cards posters and many other items.

The NFC forum (www.nfcforum.org) was formed in 2004 aimed at standardizing NFC technology. It defines NFC as: NFC is a short-range wireless connectivity technology (also known as ISO 18092) that provides intuitive, simple, and safe communication between electronic devices. Operating at the frequency of 13.56 MHz and limited short range communicating distance, NFC supports data rate of 106 Kbps, 212 Kbps and 424 Kbps. Therefore, NFC is suitable for transmission of short information or messages within small time interval.

In recent days, NFC technology is being widely popular among mobile phone vendors and related fields. This is because NFC is compatible with already existing popular technologies such as RFID, smartcards and contactless cards. It means that stores and systems equipped with the existing technologies should not replace their infrastructure in order to support NFC.

The incorporation of NFC into mobile devices has augmented capability of mobile phones and it is predicted to have potential to do more. This phenomenon has brought forward various works in terms of NFC transactions. At the same time, however, there are serious concerns in different terms such as privacy, user satisfaction, speed, usability, etc. Moreover, it is replacing various popular devices such as RFID tags. Hence, it is important to evaluate the performance of NFC technology and where it stands. In this paper, we have presented the brief insight to NFC technology and analyzed its performance as a mobile payment solution in terms of various factors. The mobile payment means passing of funds to vendor/merchant by customer to confirm the payment. The term mobile is used to represent the means to be able to move freely and easily.

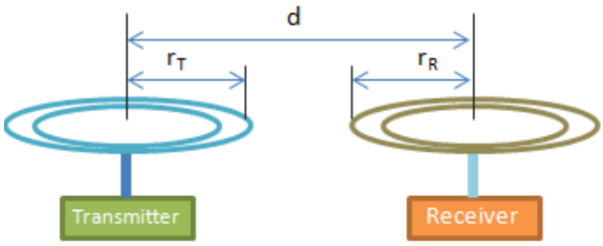


Fig. 8. A complete sound packet.

NFC devices communicate through the magnetically induced signals. Therefore, duringtransmission, energy is coupled between transceivers instead of electromagnetic radiation as in traditional wireless communication. The magnetic induction is discussed in detail in []. The magnetic induction theory

and its application to NFC are also discussed. Figure 4 shows inductively coupled NFC antennas separated by short distance usually in the units of centimeters. Within close proximity, information can be exchanged between these transceivers by magnetic induction. Equivalent circuit diagram of these antennas is shown in Figure 5.Mathematical derivation of power at the receiver for given circuit is derived in [2], where power at the receiver can be expressed as

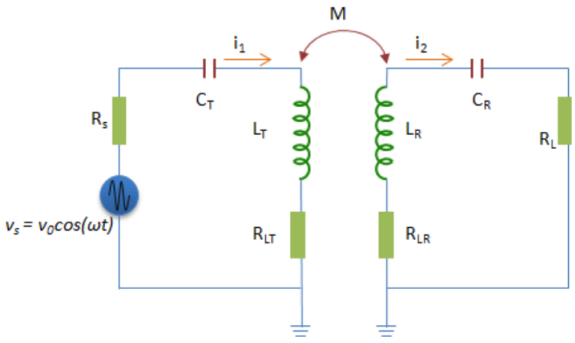


Fig. 9. A complete sound packet.

$$P_R(\omega) = P_T Q_T Q_R \eta_T \eta_T (r_T^3 \mu_0 \mu_R r_R^3 \mu_0 \mu_R \pi^2)/(r_T^3 + d^2)^3.$$

where

P_T :Transmission power,

Q_T, Q_R : Q-factors of transmitter and receiver antenna,

η_T, η_R : Efficiency of transmitter and receiver antenna,

r_T, r_R : Efficiency of transmitter and receiver antenna,

μ_0 : Radii of transmitter and receiver antenna coil,

μ_r, μ_R : Permeability of air (=1),

D : Relative permeability of transmitter and receiver antenna coil core, and Distance between transmitter and receiver antenna.

An NFC system basically consists of three components as shown in Figure 5. This is the typical casewhen an NFC phone reads an NFC tag and communicates with the backend server [3-5]. In some cases, NFC tag can be another NFC phone or also there would be no need to contact backend server [6-7]. In essence, an NFC mobile system consists of an NFC tag, an NFC chip embedded mobile phone and a backend server.

The security of NFC can be confirmed to some extent. However, as it is a wireless technology, some security issues are inevitable [12-13]:

1,Eavesdropping : Through eavesdropping, an attacker can receive the transferred information using a suitable antenna.For NFC attack, this antenna should be close enough. But, there is no solid analysis on accurate range for possible attack as it depends on attackers' antenna parameters. It is to be worth noted that NFC provides no defense mechanism against eavesdropping. In literature [8], it is discussed that eavesdropping in NFC is difficult if a device is working on passive mode. Hence, operating on passive mode could be one of the countermeasures against eavesdropping. However, it is not practical for an NFC device to always operate on passive mode. Therefore, eavesdropping can be avoided by establishing a secure channel between the devices.

2,Data Modification If the attacker has enough knowledge of the transmission, such as the mode of operation, the modulation technology used, etc., then different RF fields can be used to tamper with the data. This attack can be further divided into the following three types[14]:

1) Data Alteration: The attacker sends a valid but modified data to the receiver.

2) Data Insertion: The attacker inserts its data shortly before the receiver acknowledges the transmission.

3) Data Destruction: The attacker destroys or blocks the transmitted data so that it cannot be read by the receiver (DoS attack).

For data modification, the attacker should generate his own RF field based on the modulation and transmission techniques used by the NFC device. This is very difficult from the perspective of the attacker. In addition, NFC devices can operate in full-duplex mode. This means they can check the RF field generated by the attacker to avoid collisions.

3,Man in the middle Attack: The attacker receives the signal from the transmitter and modifies or modifies the data and sends it to the receiver and vice versa. Although this is a big issue in large-scale network security, NFC is very difficult or almost impossible because the transceiver can detect the radio field during communication and can know the unknown RF field or collision.

However, the three major mainstream payments using NFC payment now are Samsung Pay, Apple Pay, and Google pay. Its essence of TOTP technology, in the middle of the attack, will reveal a great security risk. These are mentioned in section 5.

Lost devices and abandoned connections NFC-enabled mobile devices are easily lost. However, they contain important information such as credit cards and personal data. Therefore, anyone who finds missing devices can use it just like using a lost credit card. In this case, manual security in the mobile device is the only solution, such as secure access to the phone through some PIN code or personal identification number.

On the other hand, short NFC communications can be abandoned without closing after use. These abandoned connections can be used by attackers for a variety of purposes. Therefore, communication timeout techniques should be implemented to avoid such attacks.

An NFC system basically consists of three components as shown in Figure 5. This is the typical case when an NFC phone reads an NFC tag and communicates with the backend server [4-6]. In some cases, however, NFC tag can be another NFC phone or also there would be no need to contact backend server [7-8]. In essence, an NFC mobile system consists of an NFC tag, an NFC chip embedded mobile phone and a backend server.

An NFC tag is generally embedded in items (from which it can be read) such as smart posters [4],POS, electronic devices, etc. It is a small chip usually hidden behind a sticker with NFC logo on it in order to make users aware of its existence. These tags usually contain small data based on their applications such

	NFC	Bluetooth V2.1	IrDA
Information transmission	Coupling of magnetic field	Electromagnetic radiation	Infrared light
Operating frequency	13.56 MHz	2.4 GHz	~ 2MHz?
Modes	Active-active, active-passive	Active-active	Active-active
Transmission range	0.04 – 0.1 m	10 – 100 m	0 – 2 m
Network type	P2P	WPAN (scatternet)	P2P
Maximum data rate	424 kbps	2.1 Mbps	16 Mbps
Setup time	<0.1s	~6s	~0.5s
Maximum current consumption	<15mA	<30mA	<5mA
Line of sight	Yes	No	Yes
Authentication and encryption	Yes	Yes	No
Cost of device	Low	Moderate	Low

Fig. 10. Comparison of NFC and other PAN technologies

as uniform resource identifiers (URIs), contact information, authentication credentials, valuable information, etc.

NFC chips are embedded within mobile hand-sets enabling them to read NFC tags. Mobile phone industry has shown several NFC mobile phones manufactured in last few years. It is also possible to include NFC chip within Subscriber Identity Module (SIM) card or even in micro SD cards. Therefore, hand-sets manufactured without NFC chips from industry can also be made NFC-equipped by inserting NFC-SIM or NFC-micro SD cards.

The NFC phones have several applications installed to utilize NFC capabilities based on the implementation of the system. It can also emulate existing cards such as credit cards, point cards, identity cards etc to give experience of these traditional schemes within a single mobile phone. Hence, a user is give experience of having 'everything' within their mobile device.

NFC phone could communicate to the backend server through different mobile communication technology. Service provided by the backend server might vary according to applications. For an instance, it could be a simple web page for reserving movie ticket, issuing receipts, or highly secure financial transaction service. Therefore, communication between handsets and backend server needs to implement secure connection.

Similar to RFID, NFC can also communicate on active/passive mode [9]. This means that an active NFC device is the one with power supply and generates radio field. The NFC device working on passive mode gets power supply through the active devices radiation. On the other hand, both the NFC devices can also work in active/active mode where both the devices are active devices with their own power supply. Generally, NFC can operate on three modes [4].

An NFC enabled phone acts as a tag or a kind of contactless card in card emulation mode. These tags can be read by existing traditional card readers. For an instance, it can be used as an identity card at school or office to unlock door, activate personal devices such as PC, printers, etc. Also, most common usage would be to emulate credit cards or points cards which can be used at POS terminals for payments.

An NFC has a predefined data format called NDEF data format. When an NFC phone is in read/write mode, it can read from or write data to supported tag types. Particular example usage of read/write mode is to access URI from smart posters, download short manuals of electronic devices, check out bus - arrival information at bus stops, etc.

The peer to peer mode adds quality functionality to NFC phones. In this mode, two NFC phones can exchange data with each other when brought to close proximity. For an example, two business partners can transfer their virtual business cards with each other by bringing their NFC-enabled phones close to each other. Another popular usage is for connection handoff to other standard technology; NFC connection can be used to set-up Bluetooth pairing or Wi-Fi setup. After successful setup, the handset can use the Bluetooth or Wi-Fi connections.

Fig. 11. NFC in active/passive mode

C. MST

Magnetic Secure Transmission (MST) is a technology that can transmit magnetic signals that simulate the magnetic stripe on a traditional payment card. The MST sends a magnetic signal from your device to the reader of the payment terminal (simulating the physical card swiping without upgrading the terminal's software or hardware). Almost all payment terminals with card readers can use MST technology. Some payment terminals may require software updates. Simply select a card from Samsung Pay and transfer the payment information by moving the device within one inch of the payment terminal. Your transaction and payment information will use tokenization for privacy and security. MST is more secure than using traditional payment cards and is as secure as using Near Field Communication (NFC) payments.

The technology was developed and patented by LoopPay. Samsung previously acquired the company to deploy its Samsung Pay service.The biggest highlight of Samsung Pay and Apple Pay is support for magnetic stripe card payments.

Figure 3 shows the components of the payment accessory that LoopPay made for Samsung. By using AC current, the coil will generate a magnetic field.If the correct magnetic field is generated, the coil can communicate with a credit card reader.In fact, the principle of MST is to emit a magnetic field.

However, payment security is not solved by a copper coil.The MST application has three protection mechanisms: Payment Tokenization, eSE (hardware security module) bank card information protection, KNOX, and fingerprint/password authentication.

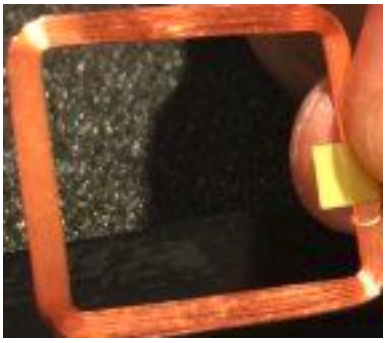


Fig. 12. token service provider

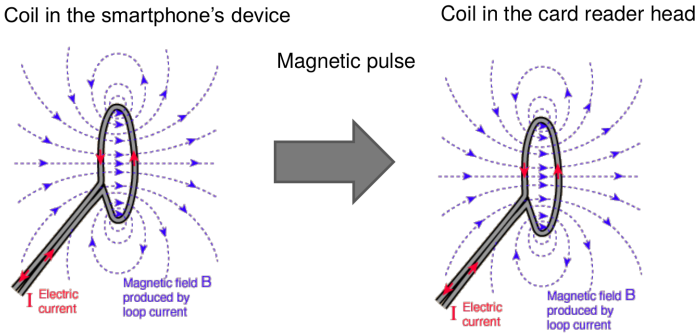


Fig. 13. Emitting magnetic pulse.

For Token, the user needs to enter the card information and send it to the card organization for verification. After the card organization passes the verification, a token will be generated for this card and the token will be sent to the device. The credit card information is not directly stored on the device. Token is stored in an independent security chip (SE chip) and used to replace the bank card number. It can be understood that the Token and the bank card number are equivalent, but even if the Token leaks, the bank card information cannot be reversed. Only when fingerprint or password authentication passes can the token be read out through the MST. Token's storage and management is governed by Samsung's own KNOX security platform.High-risk behaviors such as equipment modification occur, and KNOX can invalidate sensitive data on the device.

In other words, when using Samsung Pay's magnetic card payment mode, the key technical step is how this Token is sent. The MST generates a dynamic magnetic field through an induction coil and can be changed according to the user-defined time limit. If your mobile device is within 3 inches of the reader, you will be able to identify the magnetic field.

Like a traditional credit or debit card, magnetic fields include your payment information. The magnetic field only exists when the user chooses to send the payment information, and the magnetic field will automatically disappear once the distance between the mobile device and the reader exceeds 3 inches. This means that the attacker must be very close to the payment process to steal the payment data.

Near Field Communication (NFC) allows two devices to be located a few inches apart to exchange information. NFC payments require merchants to upgrade old terminals to NFC-enabled payment terminals. Magnetic Secure Transmission (MST) Sends magnetic signals from compatible devices to the payment terminal's reader (emulates card swiping physical payment cards). The MST payment does not require the merchant to upgrade the payment terminal so that Samsung payment can be used on almost all payment terminals with a card reader. Some payment terminals may require software updates. Samsung Pay uses NFC and MST to send payment information to the terminal. Whether using NFC or MST, transactions are seamless, providing a better user experience. Both technologies are equally secure, using a unique digital card number instead of the actual payment card number. Your information is confidential and secure. Only the payment network of your bank and credit card will provide transaction information.

D. Audio

The audio protocol we are talking about today for sonic communication is generally from the technical documentation of chirp which is a novel application for "transmitting" files via voice issued by the American startup Animal Systems.

Acoustic wave transmission is a set of technical solutions that use sound to achieve fast transmission of files: Cross-platform technology is used to implement data transmission between any device that can send sound waves and receive sound waves.There are also a large number of applications in mobile payments.

1) encoding: The principle of the audio protocol is simple and easy to implement. Create a table with 32 characters and map each character to a frequency table. The frequency table is generated based on the music theory through the calculation of sound.Each character is represented by the pitch of one frequency, so there are 32 frequencies, 0 corresponds to 1760 Hz, 1 corresponds to 1864 Hz,..., v corresponds to 10.5 kHz, and the adjacent frequency differs by a half interval.

The audio produced by Chirp contains 20 characters. Each character is generated with a sine wave of the corresponding frequency. Each sine wave lasts 87.2 ms. If the sampling rate is 44.1 kHz, then each character is about 3846 samples. The whole audio is about 20*87.2ms=1.744s, because each character is represented by a different frequency, it sounds like music.

A complete sound packet contains 20 tones (ie 20 characters), one tone every 87.2 milliseconds. The first two bits are headers and use hj to notify the receiver to start receiving. The middle 10 bits are valid information bits, which are effective transmission information, that is, Key values are mapped after the frequency information. The last 8 bits are the RS check digits. The RS parity check algorithm calculates the middle 10 bits and generates 8-bit parity information.

2	10	8
information header	data bits	RS validity bits

Fig. 14. A complete sound packet.

2) decoding: Chirp describes the technical details of relying on sound for data communication between a smart device, but in fact, the audio protocol of the sound wave communication can be arbitrarily designed by itself, for example, changing the sound in the chirp audio protocol to double-frequency sound, even multi-tone sound. In order to increase the information capacity per unit time, thereby increasing the transmission speed, this is all possible, as long as there is a demand for this application.

The receiver needs to record the sound and perform it and fault-tolerant processing. Its relatively high requirements on the algorithm, noise reduction and fault-tolerant processing are critical to the correct information

IV. ONLINE PAYMENT TECHNOLOGIES

Internet transfer payment technology, as the name suggests, is a transfer payment via the Internet.Different from the PC terminal, the network transfer payment at the mobile terminal needs to pay for the support of the client's app.

Network transfer payment technology is mainly based on the security of tokenization technology.

A. scan the QR code

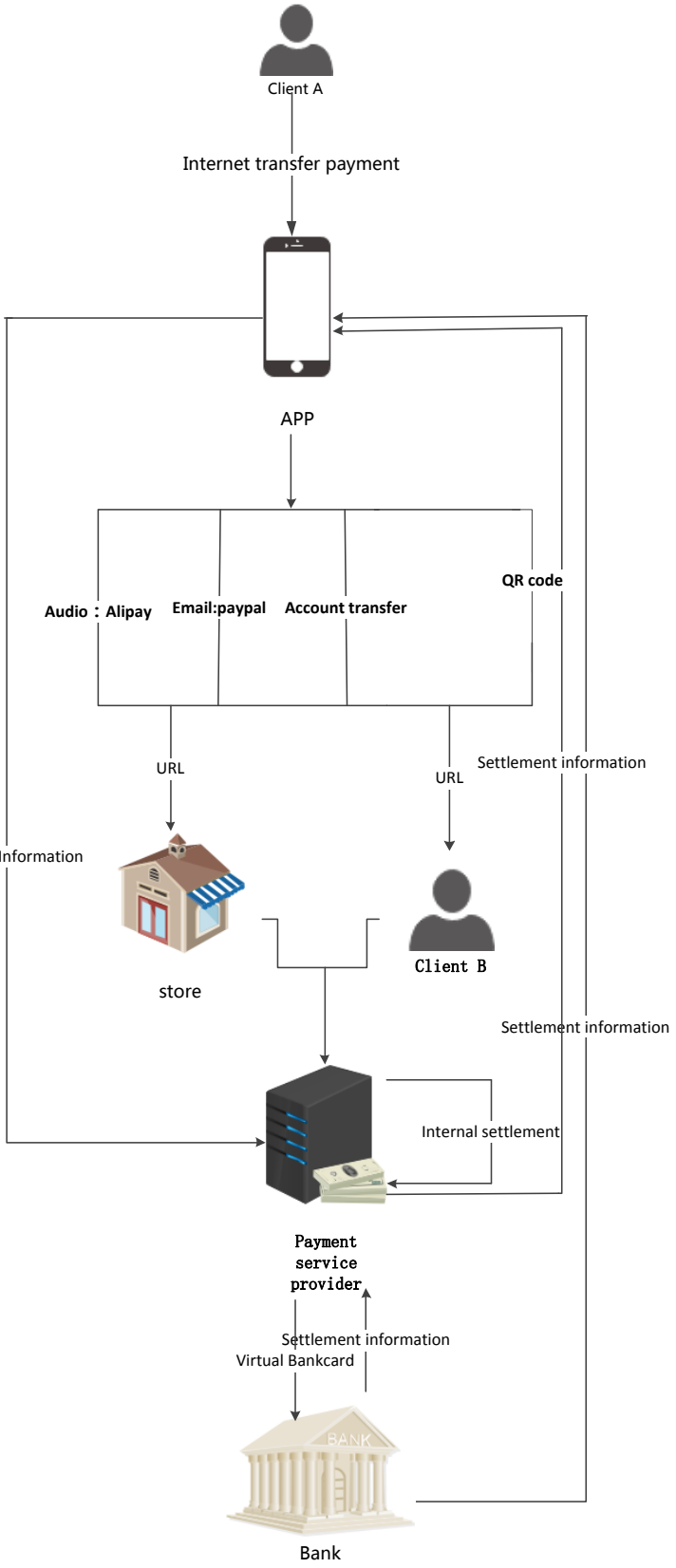
In the scan code payment scenario, the QR code is actually a url with some parameters. The scan code will initiate the transfer. The two-dimensional code is actually only an account medium, a data storage body, which itself is not the result of the payment innovation. The existing various QR code payment only replaces the data carrier of the original payment means with a two-dimensional code. Similar chip content with bank cards. Is an account of the embodiment.

B. Through email

V. OFFLINE PAYMENT TECHNOLOGIES

Offline payment is a payment method which the most prominent feature is that the paying party do not need connecting to the Internet, which means only one party need communicate with the payment server.It is widely welcomed due to its ease of use. In China today, this type of payment method can be seen everywhere, from large shopping malls to small supermarket chains. Even in the underground shopping malls with poor network signals, the surrounding areas of the city, and tourist attractions in the mountains, as long as a mobile phone in hand, you can pay for you.

Off-line payment is mainly provided by two major technologies, one mainly provided by large-scale payment service providers such as Alipay, Tencent, UnionPay, Wal-Mart, and Amazon. It mainly binds the bank card to the account of the corresponding payment provider and uses the TOTP technology to generate the payment password and use the account number to pay. Another source is mainly provided by large mobile terminals or system providers, such as Apple, Samsung, and Google. It mainly binds the bank card to the mobile phone terminal and simulates the bank card payment method and pays for direct connection to the bank.



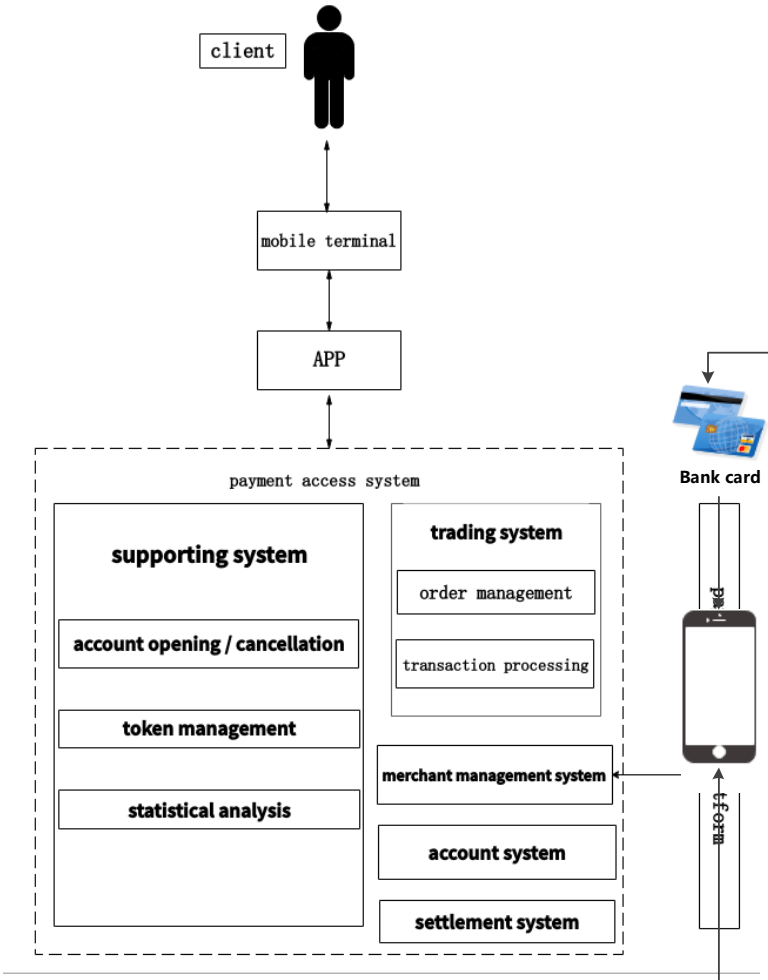


Fig. 16. App payment.

Figure 15 shows the entire process of offline payment from client to bank, including TOTP payment represented by Alipay and analog bank card payment represented by Samsu

First look at the former, after the TOTP is generated by the mobile phone, the QR code or audio is used as a carrier to the store. The store transmits the TOTP plus payment information to the server of the payment service provider, decodes the TOTP and completes the settlement. At this time, the payment provider The money in the customer's account in the database is transferred to the store's account.

A. *Time-Based One-Time Password:The key to offline payment*

one of the technical prototypes of the off-line payment is a one-time password (OTP) widely used in the industry. Products using this technology include Alipay and WeChat, as well as hardware equipment such as bank U shields and game tokens.

Regardless of Alipay or WeChat, they scanned the payment using 18-digit digitally-generated barcodes and QR codes. This 18-digit number is the payment password.

1) HMAC(Message Authentication Code Algorithm Based on Hash Function): Algorithm formula:

$$HMAC(K,m) = H((K'xoropad)||H((K'xoripad)||m))$$

- H:hash functio4;

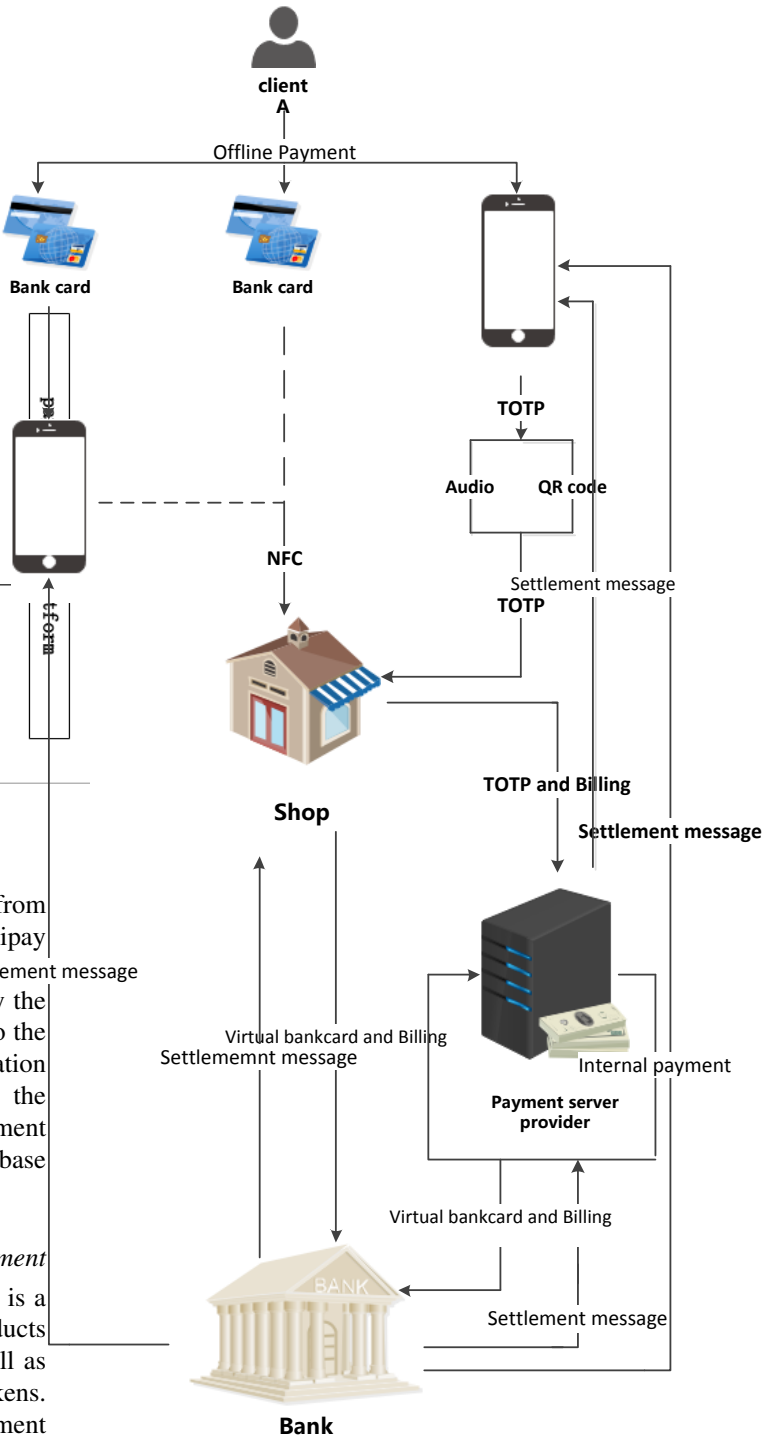


Fig. 17. Offline payment.

• K:shared secret key;

•:K' calculated by K(key) (The hash function of this scheme is SHA-1, MD5, RIPEMD-128/160, and the size of K' is 64 bytes, followed by 0);

• xor;

• opad:outer HASH padding value, 0x5c5c5c.... Length equal to K K';

• ipad:inner HASH padding value, 0x363636.... Length equal to K';

• m:a message input;

• ||:Indicates connection.

2) HOTCP(HMAC-based One-Time Password): Algorithm formula:

$HOTP(K,C) = (Truncate(HMAC(K,C))\&0x7FFFFFFF) mod 10^d$

• C:counter;

• Truncate:after processing will get a 32bit unsigned integer;

• A d-bit numeric password is obtained with a d-squared modulus operation of 10.

3) TOTP(Time-Based One-Time Password): Algorithm formula:

$$TOTP = HOTP(K, TC)$$

• $TC = f((unixtime(now)unixtime(T0))/TS)$;

• T0:The time step to start the calculation;

• TS:Time Step.

After the terminal installs the client and starts the application for the first time, the server can generate a unique token and the device ID corresponding to the token.

• Token: The seed used to generate the OTP code.

• Device ID: Used to uniquely identify the terminal.

After sending the token and the device ID to each terminal, the server needs to store the mapping relationship between the token and the device ID.

The terminal calculates the dynamic password by using the pre-stored token and the current time as input values of first preset algorithm.

The first preset algorithm may be an arbitrarily for irreversible algorithm

1, time synchronization algorithm (TOTP);

2, event synchronization algorithm (HOTP);

3, challenge response algorithm (OCRA);

Alipay and moust of payment server provider now mainly uses TOTP technology

The first information can be any of the following:

1, dynamic password: such as: 123456.

2, the combination of dynamic password and current time value: such as: 123456 (dynamic password) 20160503110232 (current time value)

3, device ID and dynamic password:

4, device ID and dynamic password + current time value.

The first information including the above-mentioned dynamic password is used as the input value of the second preset algorithm, and the second information is calculated.

The second preset algorithm is an irreversible algorithm such as: HMAC, MD5, or HMAC-SHA algorithm.

second information is generally obtained with the token and the first information as input values

1, find the corresponding token with the device ID of the authentication password

2, using the token and the first default algorithm to verify the dynamic password. The trusted dynamic password list is first calculated (the trusted dynamic list includes multiple trusted dynamic passwords). If it is found that a certain trusted dynamic oral delivery is consistent with the above-mentioned dynamic password, the dynamic password verification passes.

3, using the first information and the second preset algorithm to verify the second information

10: device ID

20: Dynamic password

30: second information

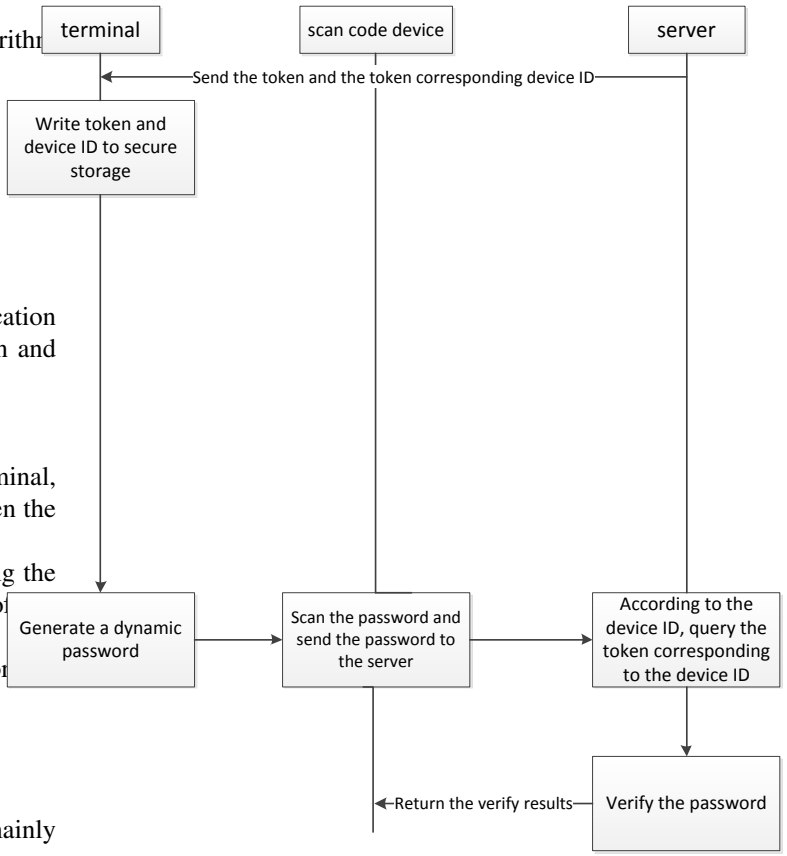


Fig. 18. Time-Based One-Time Password.

B. IC card and its imitation payment

IC card credit card payment is the main portable payment method before mobile payment. Especially in Europe and the United States, it has become a payment method that many people have become accustomed to. Therefore, Samsung, Apple, Google and other large European and American Internet

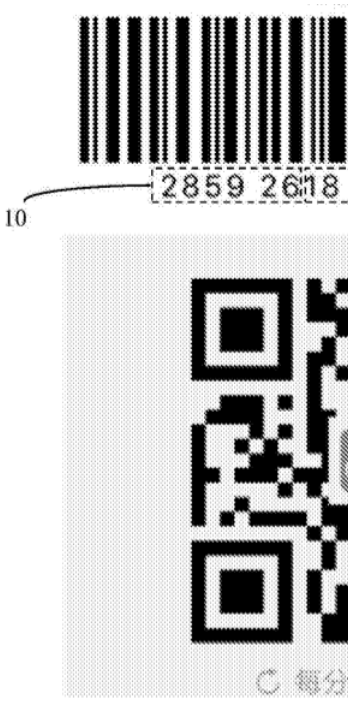


Fig. 19. Offline payment.

companies have taken a diffe
Alibaba and Tencent when t

Different from the use of
and other means. They work
mitted to using mobile phor
which hope to have a swipe

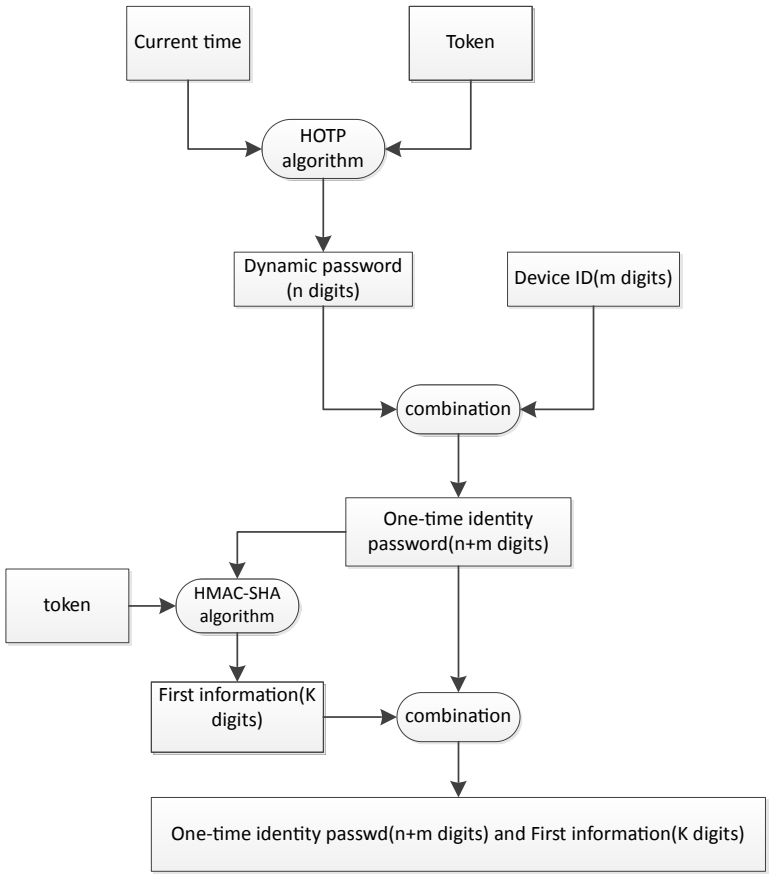


Fig. 20. Time-Based One-Time Password.

C. bank card

The bank card is divided by the interface and can be divided into:

magnetic card;

IC card (chip card).

1) magnetic card: A magnetic card is a card-like magnetic recording medium that uses magnetic carriers to record characters and digital information for identification purposes or other purposes. The magnetic card is made of high-strength, high-temperature-resistant plastic or paper-coated plastic, and can be damp-proof, wear-resistant and have certain flexibility. It is easy to carry and uses more stable and reliable. For example, the bank card we used before is the most common magnetic stripe card.

The magnetic stripe card is a veteran of the card industry. It has the longest usage time and the largest number of uses. With the development of informatization and electronic technology, magnetic stripe cards have gradually faded out of the stage of history due to the disadvantages described above.

2) IC card: An integrated circuit card (IC card) is also called a smart card, an intelligent card, a microcircuit card, or a microchip card. It embeds a microelectronic chip into a card base conforming to the ISO 7816 standard in the form of a card. The communication between the IC card and the reader can be either contact or non-contact. According to the communication interface, the IC card is divided into a contact type IC card, a non-contact type IC, and a dual interface card (having both a contact type and a non-contact type communication interface).

Because of its inherent information security, portability, and relatively standardization, IC cards are increasingly used in identity authentication, banking, telecommunications, public transportation, and yard management, for example, second-generation ID cards, and banks. Electronic purses, telecommunication SIM cards for mobile phones, bus cards for public transportation, subway cards, parking cards for parking fees, etc. all play an important role in people's daily lives.

IC card is another kind of information carrier after the magnetic card. The IC card refers to an integrated circuit card. A commonly used bus card is a kind of IC card. Generally, a common IC card uses radio frequency technology to communicate with a card reader supporting an IC card. There is a difference between the IC card and the magnetic card. The IC card stores information through the integrated circuit in the card, and the magnetic card records information through the magnetic force in the card. IC cards are generally higher in

cost than magnetic cards, but have better confidentiality.

The subdivision of chips can be divided into

contact card: Contact: only support contact transactions, transactions need to plug into the POS machine

non-contact card: Non-contact: only support non-contact transactions, trade on the POS machine, usually non-contact IC is buried in the card, the surface can not see.

dual interfaces card.: The dual interface means that the IC card supports both interfaces. Therefore, only when the bank card is an IC card that supports non-contact transactions, it is possible for the NFC terminal to read the card information.

D. Mobile phone imitate IC card

With the gradual deployment of Android Pay, Apple Pay and Samsung Pay, mobile payments have returned to the public eye and the comparative articles on several types of payment have not been uncommon in recent days. This article mainly discusses the similarities and differences between several payment methods from a technical point of view.

Apple Pay and Android Pay each serve as a system-level payment application (Apple Pay by iOS, Android Pay by Android), not only play the role of application, but also has a God perspective, as a system feature for other applications developers A unified payment gateway. In other words, other shopping and service applications can invoke APIs of Apple Pay or Android Pay in the development code to charge consumers, for example, purchasing a movie ticket. Before the application is almost always linked to VISA or MasterCard online payment allows users to fill in the cardholder name, card number, expiration date, code and other safety information, each time you have to fill in the shopping (the site should not and can not be saved), or combined with OTP (one-time password) certification, This is a hassle and a safety hazard (previously PC-based cookies were hacked, or consumer websites saved user-card information, such as previous Ctrip, resulting in theft of credit card information); application developers can now call Pay, allowing users to choose their own credit card has been added to pay, users do not need to fill in a form, a key shopping, the real charge to pay to do.

Relative to the online payment (in short, that is connected with the Internet, the payment of data through the network transmission), offline payment is a physical payment, you need a terminal device chargeback, in most cases, POS machines. In order to replace the traditional credit card with credit card spending, NFC + Pay way allows consumers to use a cell phone, rather than a variety of cards for ”flash” consumption. Pay only needs the POS machine to support NFC without any other modification. Therefore, offline entity merchants accept this payment method exactly as the acceptance of non-connected bank cards such as MasterCard Pay Pass, Visa Pay Wave, China Union Pay Flash Quick Pass , There is no promotion barriers, but also to speed up the deployment of wireless POS machines coupled with a heavy weight.

1) sumsung pay: Samsung Pay uses NFC and MST technologies.

Samsung Pay uses both NFC and MST to send payment information to the terminal. The transaction is seamless, whether using NFC or MST, allowing for a better user experience.

Both technologies are equally secure, using a unique digital card number in place of the actual card number. The information is kept private and secure, and only the bank and the card's payment network will have information on the transaction

Samsung's payment technology also uses TOTP technology and virtual bank card technology. The following steps can be known from Fig 21:

1, The client first submits bank card-related information on the app. Samsung takes them to the bank or card organization in exchange for a virtual silver card and secret value and binds it with the user account. In addition to being stored on the server, it is also stored in the KNOX of the client's mobile phone.

2, Combine the virtual line card with the secret value and add the TOTP algorithm to get a one-time payment password. The following is a guess. When the payment is made again, the first 6 digits and the last 4 digits of the password are the same as the virtual bank card. The middle 8 digits are TOTP passwords.

3,The payment password using MST or NFC encoding, and simulate the physical bank card payment method in pos credit card. The payment password and the pos machine ID are transmitted to the bank server via the payment network.

4,The bank server obtains the virtual bank card by decrypting the TOTP, and obtains the real bank card through the de-tokenization technology. Finally, the bank card is used for real payment, and the payment completion information is returned to the Samsung server.

Samsung's MST payments and NFC payments are analog bank card payments. Not only that, S and C will be displayed behind the pos card number on the pos machine.

In fact, this means that the physical card swiping method. S means the media representing the card is a magnetic stripe. I means that use the intergated chip. C and Q are the non-contact transactions.

It can be concluded that Samsung's payment, while simulating the physical card payment on the surface, essentially uses the core technologies of mobile offline payment, namely, tokenization and TOTP.

2) Android pay:

3) apple pay: Apple pays only NFC payments, and its technology is very similar to Samsung's NFC technology, but Apple's use of the scene is not Samsung. Because it does not support magnetic stripe payments, it supports Apple payments on many older devices that only support magnetic stripe payments.

By comparison, it is not difficult to see that Apple Pay and Samsung Pay have an essential difference from Chinas Alipay/WeChat. Apple Pay and Samsung Pay do not have their own account ecology. They are only used to replace bank cards for online and offline consumption, eliminating the need to carry bank cards or memories, but are limited to only

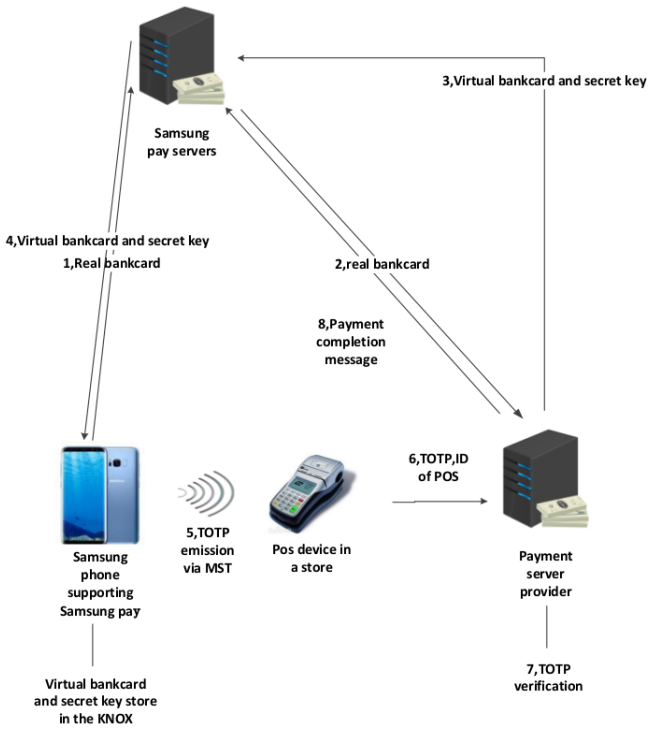


Fig. 21. samsung pay service architecture.

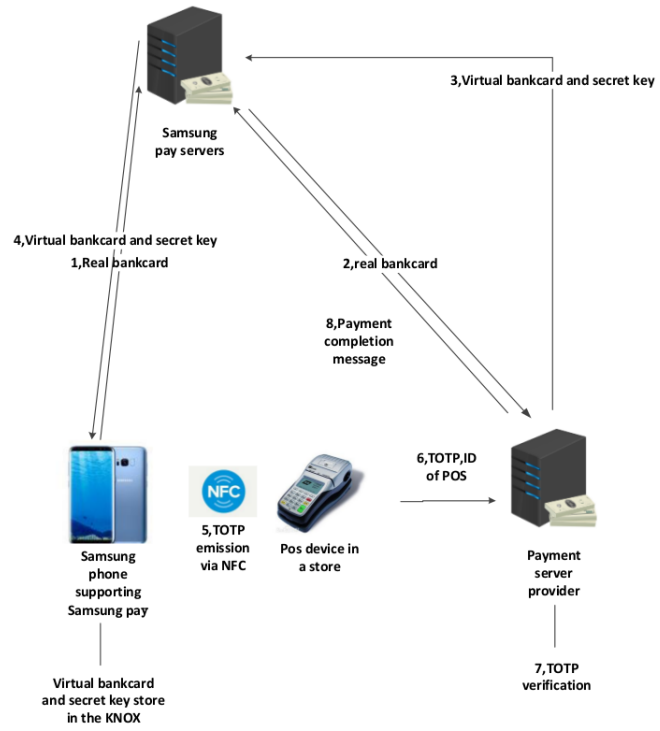


Fig. 22. samsung pay service architecture.

supporting their own models, and their audiences are relatively Narrower.

VI. Disscusion and security comparison

VII. Conclusion

The conclusion goes here.

Appendix A
Proof of the First Zonklar Equation

Appendix one text goes here.

Appendix B

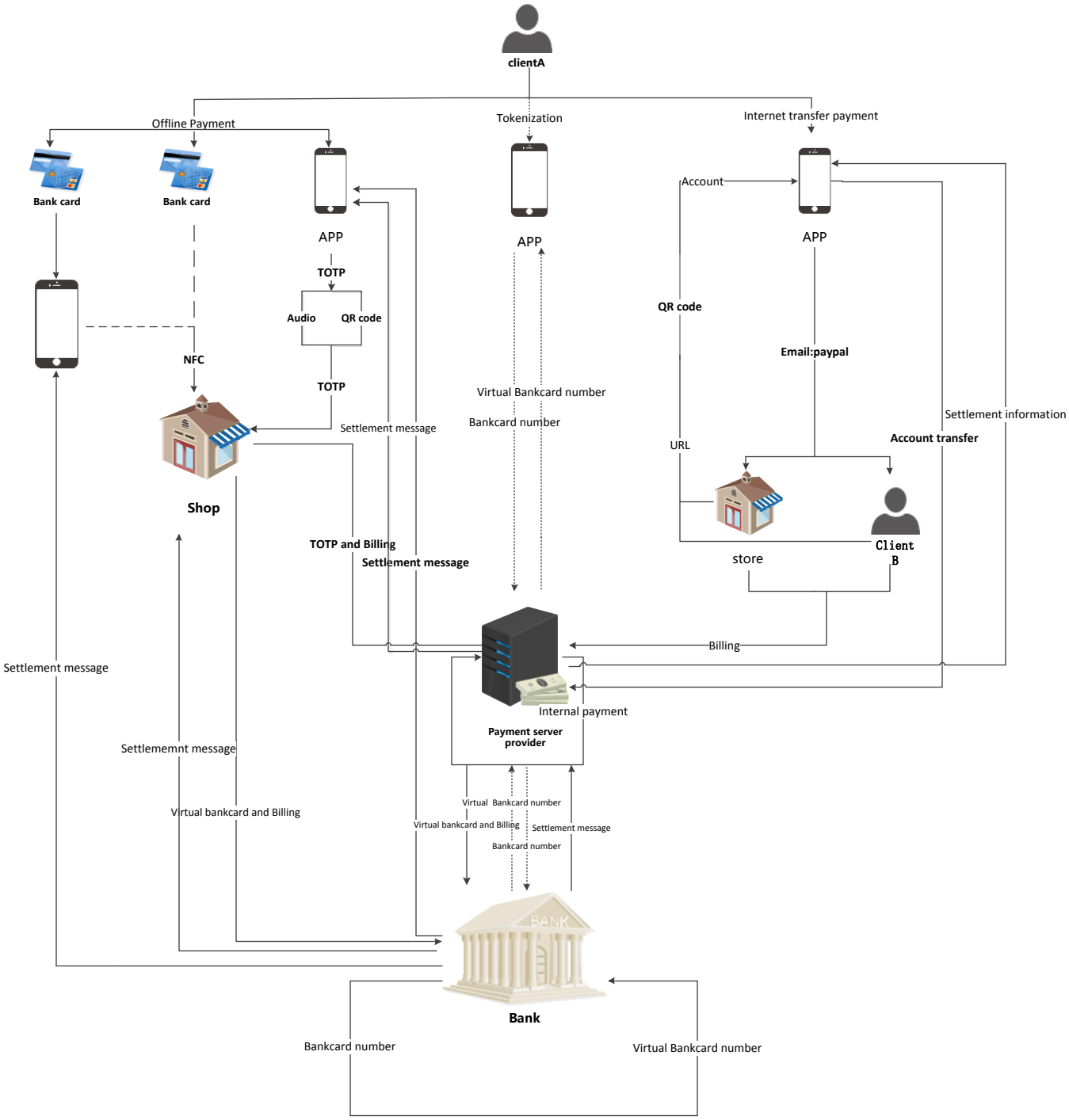
Appendix two text goes here.

Acknowledgment

The authors would like to thank...

References

[1] H. Kopka and P. W. Daly, *A Guide to LaTeX*, 3rd ed. Harlow, England: Addison-Wesley, 1999.
[2] Agbinya J I, Masihpour M. *Power Equations and Capacity Performance of Magnetic Induction Communication Systems[J].* Wireless Personal Communications, 2012, 64(4):831-845.
[3] Timalsina S K, Moh S. A review on NFC and NFC-based mobile payment solution[J]. Journal of Next Generation Information Technology, 2012, 3(4):35-44.
[4] NFC Forum, *White paper on smart posters*, Tech. Rep., Apr. 2011.
[5] NFC Forum, *White paper on essentials for successful NFC mobile ecosystem,* Tech. Rep., Oct. 2008.
[6] NFC Forum, *White paper on the keys to truly interoperable communications*, Tech. Rep., Oct.2007.
[7] R. Steffen, J. Prei andinger, T. Scho andllermann, A. Mu andller, and I. Schnabel, *Near field communication (NFC) in an automotive environment,* Proc. of 2010 Second International Workshop on Near Field Communication (NFC), pp. 15-20, Apr. 2010.
[8] E. Haselsteiner and K. Breitfu, *Security in near field communication (NFC),* Proc. of Workshop on RFID security, 2006.
[9] E. Haselsteiner and K. Breitfu, *Security in near field communication (NFC),* Proc. of Workshop on RFID security, 2006.
[10] PCI Security Standards Council. Information supplement: PCI DSS tokenization guidelines, 2011. Available at "https:www.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf".
[11] Daz-Santiago, S., Rodriguez-Henriquez, L. M., & Chakraborty, D. (2016). *A cryptographic study of tokenization systems.* International Conference on Security and Cryptography (Vol.15, pp.413-432). IEEE.
[12] E. Haselsteiner and K. Breitfu, *Security in near field communication (NFC),* Proc. of Workshop on RFID security, 2006.
[13] C. Mulliner, *Vulnerability analysis and attacks on NFC-enabled mobile phones,* Proc. of International Conference on Availability, Reliability and Security (ARES 09), pp. 695-700, Mar.2009.
[14] Timalsina S K, Moh S. *A review on NFC and NFC-based mobile payment solution[J].* Journal of Next Generation Information Technology, 2012, 3(4):35-44.


clientA
Offline Payment
Tokenization
Internet transfer payment
Bank card
Bank card
APP
APP
APP
Account
TOTP
Audio
QR code
QR code
NFC
Email:paypal
Virtual Bankcard number
Bankcard number
Settlement information
Settlement message
URL
Account transfer
Shop
store
Client B
TOTP and Billing
Settlement message
Billing
Settlement message
Internal payment
Payment server provider
Settlememnt message
Virtual bankcard and Billing
Virtual Bankcard number
Virtual bankcard and Billing
Settlement message
Bankcard number
BANK
Bank
Bankcard number
Virtual Bankcard number

Michael Shell Biography text here.

John Doe Biography text here.

Jane Doe Biography text here.