A Survey of Technologies for Mobile Payment Security

Wenzheng Liu, *NUDT,* Xiaofeng Wang, *NUDT,* Wei Peng, *NUDT,*

***Abstract*—With mobile payments popular all over the world, people almost no need to bring a wallet, the bank card is stored directly in the mobile phone and also allows the users to conduct a payment anytime and anywhere. While providing convenience to people, it also brings more payment security issues. This paper carefully discussed the overall technical framework of payment and conducted a layered analysis of the entire payment process from the mobile phone to the bank. classifies mobile payment and gives the structure and model of the mobile payment system. Discussing mobile payment security from the perspective of security technology, involving secure payment token technology, secure payment mobile terminal technology, secure payment authentication technology, secure payment communication technology. Finally, from the perspective of security technology mentioned above to analysis today's mainstream mobile payment solutions such as Alipay, Wechat pay, Samsung pay, Google pay and Apple pay are analyzed, The main features and security discussion are held for each scheme, pointing out the respective deficiencies and directions for improvement.**

***Index Terms*—tokenization, eSE, QR code, NFC, offline, TOTP.**

I. Introduction

Since modern times, payment methods have tremendous changes. People began to pay in cash. Then, technology deposits cash into magnetic stripe cards and IC cards. Thus people (especially in Europe and the United States) gradually fond of paying by their cards, but today's technology again puts bank cards into mobile phones. mobile payments have become a general trend. Today, mobile payments are beginning to dominate the market worldwide. In China, from luxury shopping malls to simple roadside stalls, there are almost no places that do not support mobile payments. People go out without cash, take the bus and subway swiped mobile phones, and simply scan the QR code for dining and shopping. In Europe and the United States, mobile phones continue to perform credit card operations as a substitute for bank cards. Samsung, Google and Apple have joined MasterCard, Visa and other card organizations to promote their respective payment programs, almost every mall can see the logo of Samsung pay, Google pay, Apple pay. In other parts of the world, mobile payments are also slowly entering peoples lives, regardless of poverty and wealth. The day it completely occupied the market will come back sooner or later.

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.

Today's major mobile payment solutions can be divided into two camps. One party is based mainly on Alipay, Tencent, Paypal, MasterCard, etc. They are not simply payment providers, but also have some of the bank's functions. The user only interacts with the payment server. After completing the settlement within the server, the server then interacts with the bank. Therefore, the main security technology is used from the user's payment to server authentication. On the other hand, they are Apple, Samsung, Google and other mobile phone manufacturers. In order not to change people's habits of swiping cards, they use their hardware advantages to directly connect with banks and use mobile phones to simulate the entire payment process of the bank cards. Since the IC card itself is very complicated, in order to simulate its functions and maintain the same security, mobile phone manufacturers and banks have jointly developed a large number of software and hardware technologies on mobile terminals. Offline payment (that is, the mobile terminal does not need to pay for networking) is the research focus of the two camps this year. The payment service providers paid for by using the password + QR codes, quickly occupying the Chinese market with their low hardware requirements and strong compatibility. In the European and American markets, there is not enough trust in this model, and mobile phone manufacturers have also achieved the offline payment function by means of analog bank card flash payment. Then there is the security issue of the mobile terminal, ie how the mobile terminal stores sensitive information and guarantees data security in the payment process. The technologies involved are trustzone and eSE.

The security issues of mobile payments are mainly divided into several categories. The first is the bank card binding problem, that is, in what form, what way the bank card is bound to the mobile phone. The technologies involved are tokenization and bank card binding security scheme. Then there is the security issue of the mobile terminal, how the mobile terminal stores sensitive information and guarantees data security in the payment process. The technologies involved are trustzone and eSE. Finally, secure payment authentication and communication issues,how to ensure the security and authentication of mobile payments from mobile phones to banks.

In conjunction with the above-mentioned objective, the remainder of this study is organized based on the major research areas of mobile payment security: in Section 2, Introduce the structure and model of the entire mobile payment system in Section 3, we present the virtual bank card binding technology. In Section 4, Mobile terminal security technology related to mobile payment are reviewed. Section 5 contains

payment communication technologis. In Section 6 onlie payment technologies are discussed, and Section 7 introduce China's Alipay, Wechat offline technology. In Section 8 focus on the technology of using mobile phone to simulate bank card payment. Concurrently, we summarize the entire technology and analyze the advantages and disadvantages and also future development trends.

II. Mobile payment security system

In this section will introduce the entire mobile payment system structure. First introduce the process of mobile payment, also explain the related technologies and ideas involved. Grasp the entire mobile payment from a macro perspective and analyze it in detail in later sections. Mobile payment will then be analyzed from a security technology perspective, from hardware security technology to payment authentication technology.

A. Mobile payment process model

The first process to introduce is bank card binding. Different from traditional bank card payments, our PANs(bank card number) are not allowed to stored on the phone or the server of Alibaba or Samsung, or be transmitted over the network frequently. Therefore, the token is used to perform related operations instead of the real PAN.

The left and right of Figure 1 describes the bank card binding process:

1, The customer opens the payment app and enters the bank card number on the binding bank card interface.

2, The mobile terminal sends the bank card number to the server of the payment provider through the secure communication network.

3, the server interacts with the card organization and obtains the token of the bank card, saves and returns it to the mobile terminal

4, the mobile terminal will save the token

No matter which payment software you use, what is really bound to the phone is the token, which we also call a virtual bank card. This technique and its security analysis is covered in detail in the next section.

After getting the token, the phone can use it to initiate mobile payment.

In the mobile payment process, payment service providers such as Alipay, WeChat,etc are very similar to those of mobile phone manufacturers such as Samsung, Apple, etc, but the entire payment process and technology are completely different.

The right side of Figure 1 describes the payment process of Alipay, WeChat, etc. The process is as follows

1, The mobile terminal generates a time-based one-time password (TOTP) and transmits it to the PoS machine through the QR code or audio;

2, The store PoS sends the TOTP and transaction information to the payment service provider's server via a secure communication network, which will analyze the TOTP certified payment and confirm the payer;

3.1, Case 1, if the user is using account balance payment, the server will internally settle and complete the transaction,end;

3.2, Case 2, if the user is using a virtual bank card payment. The server will transmit the token and transaction information to the card organization (China UnionPay, Visa, MasterCard, etc.). After the card organization obtains the token, it can find the corresponding PAN through de-tokenization and contact the issuing bank to complete the transaction.

attention:Alipay, WeChat, etc. all have their own accounts in the bank. The process of transferring money to users' Alipay and WeChat accounts is actually transferring money to Alipay and WeChat bank accounts. So when the user pays with the account balance, the money is actually in the bank account of Alipay or WeChat and has not moved.

The left side of Figure 1 describes the payment process of Samsung, Apple,etc. The process is as follows

1, Mobile phone simulates bank card payment mode through hardware;

2, Activate payment by fingerprint or PIN, and use NFC to simulate the process of contactless card consumption to interact with PoS machine. Samsung mobile phone can also simulate the consumption of magnetic stripe card by MST.

3, The PoS obtains the TOTP generated by the token or the token and the TOTP will directly communicate with the card organization after adding the information required by other contactless cards or magnetic stripe cards.

4, After the card organization obtains the token, it can find the corresponding PAN through de-tokenization and contact the issuing bank to complete the transaction.

As can be seen from the above, Alipay, WeChat, etc. not only provide payment services for users, but also bear a certain degree of banking functions. And Samsung, Apple, etc. just to provide users with convenient payment.

B. Mobile payment security technoligies

This section mainly introduces relevant security technologies through the payment process.

The key technology at the bottom is tokenization, which is divided into centralized tokenization and distributed tokenization. The core technology of former iscentral database mapping technology, The core technology of latter isdistrubuted lookup table.

Mobile terminal security technologies are mainly trustzone and SE technologies. The former provides a secure operating environment and the latter provides secure storage.

III. Virtual Bank card binding technology

Virtual bank card instead of the real bank card binding in the mobile terminal and transfer in the transaction.In this section, the Virtual bank card binding technology will be told.

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

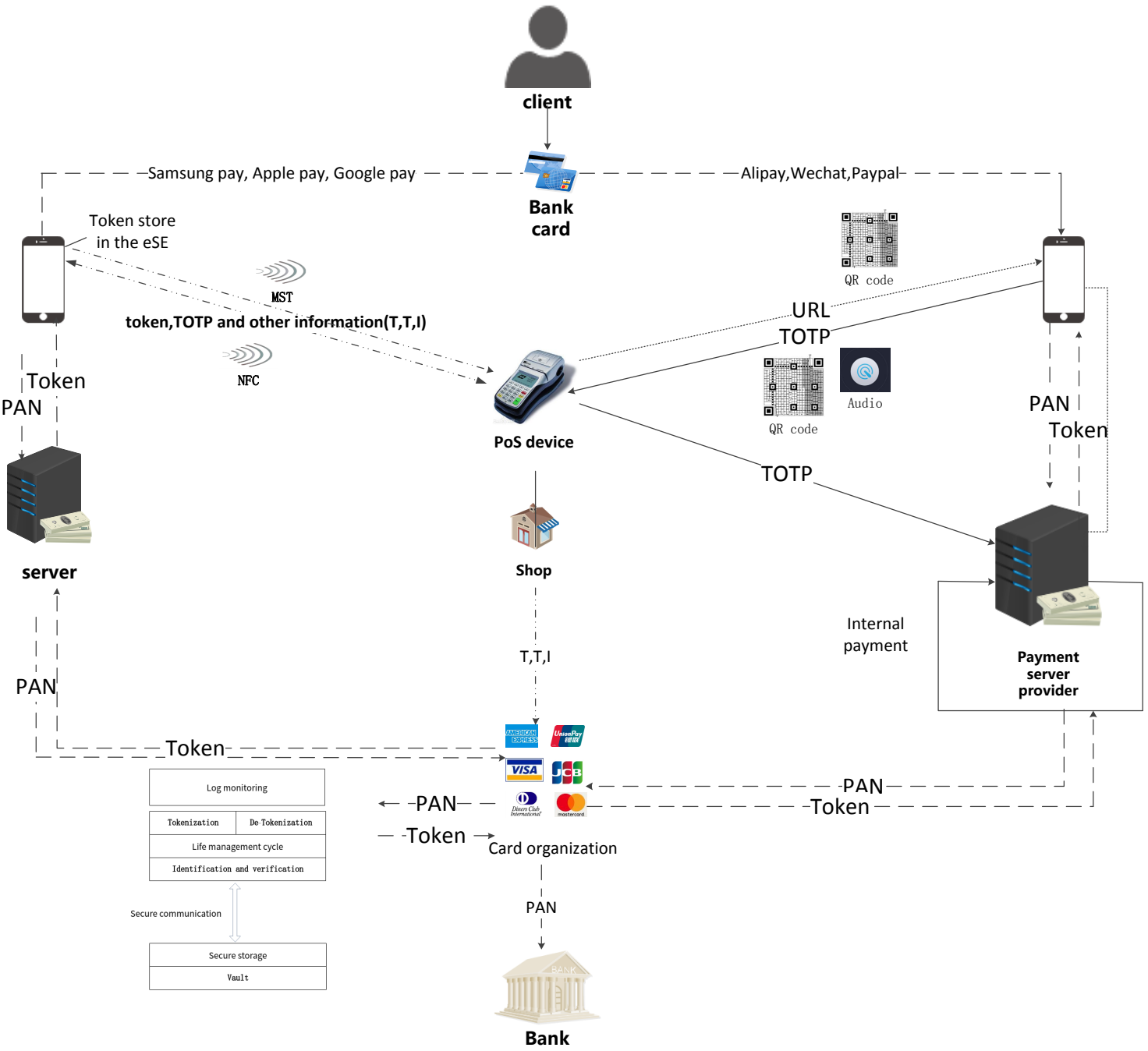

Fig. 1. Mobile payment framework.

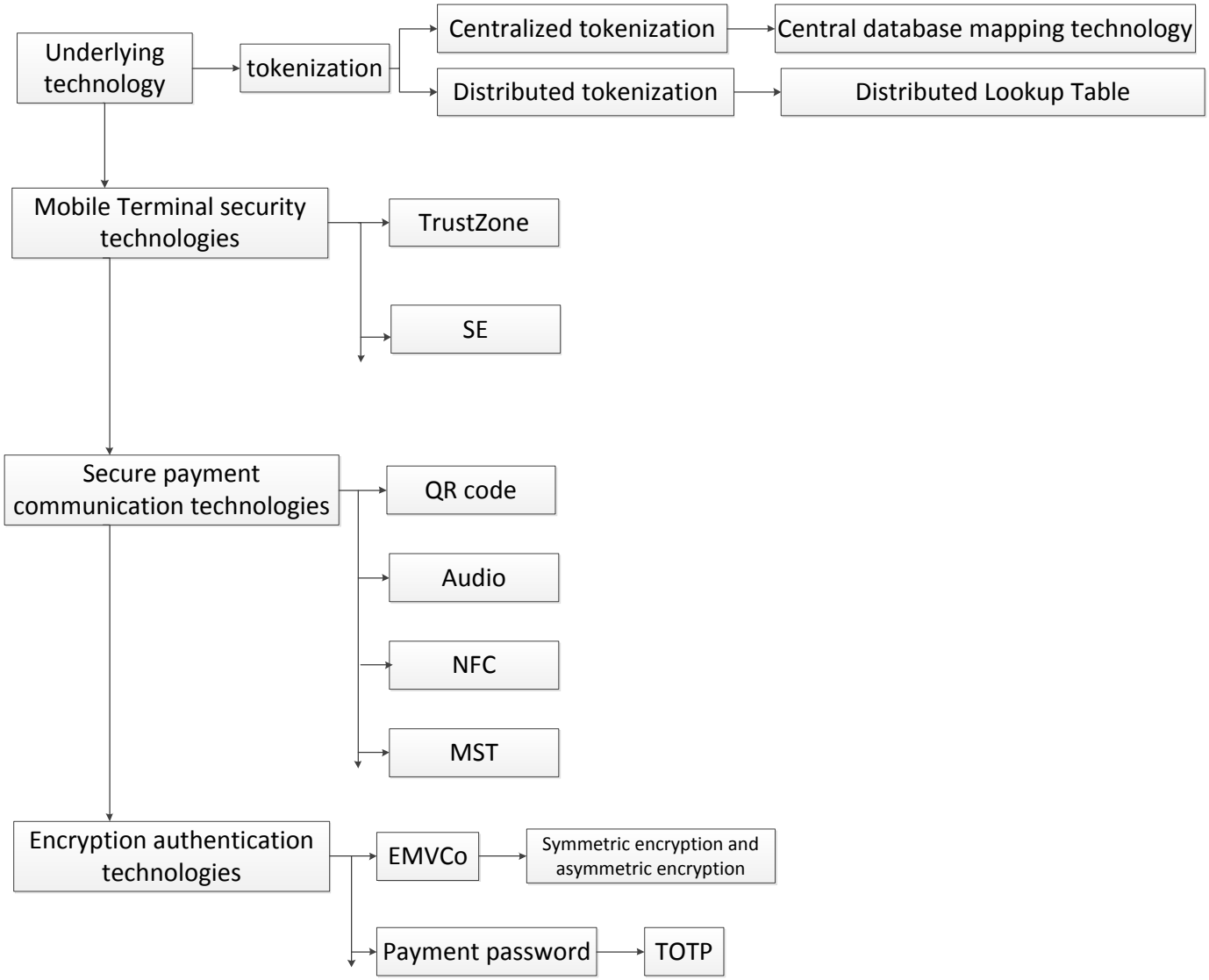

Fig. 2. Mobile payment technology framework.

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 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.

A. Fundamental of virtual bank card:tokenization

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 tokens 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.

Attention: The conception of token in the different field of computer security has a different meaning. But all have some temporary properties. In identity authentication, when the user logs in for the first time, the server generates a token and returns the token to the client. After that, the client only needs to bring the token to request data, without having to bring the user name and password again. Besides, token is also an object used in Petri net theory. Not only that, there are Access token(a system object representing the subject of access control operations), Session token (a unique identifier of an interaction session), Security token or hardware token (authentication token or cryptographic token, a physical device for computer authentication), Token ring(a network technology in which a token circles in a logical ring),etc. Many people confuse the token in the payment security with the token in the authentication, and believe that the payment can be authenticated as long as the token is presented. This is actually wrong. In the field of mobile payments, Tokenization is the process of substituting a sensitive data element. The token is stored in the mobile terminal instead of the PAN.

The international chip card standardization organization EMVCo has defined smart card payment and also defined a 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, 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 and random 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 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.

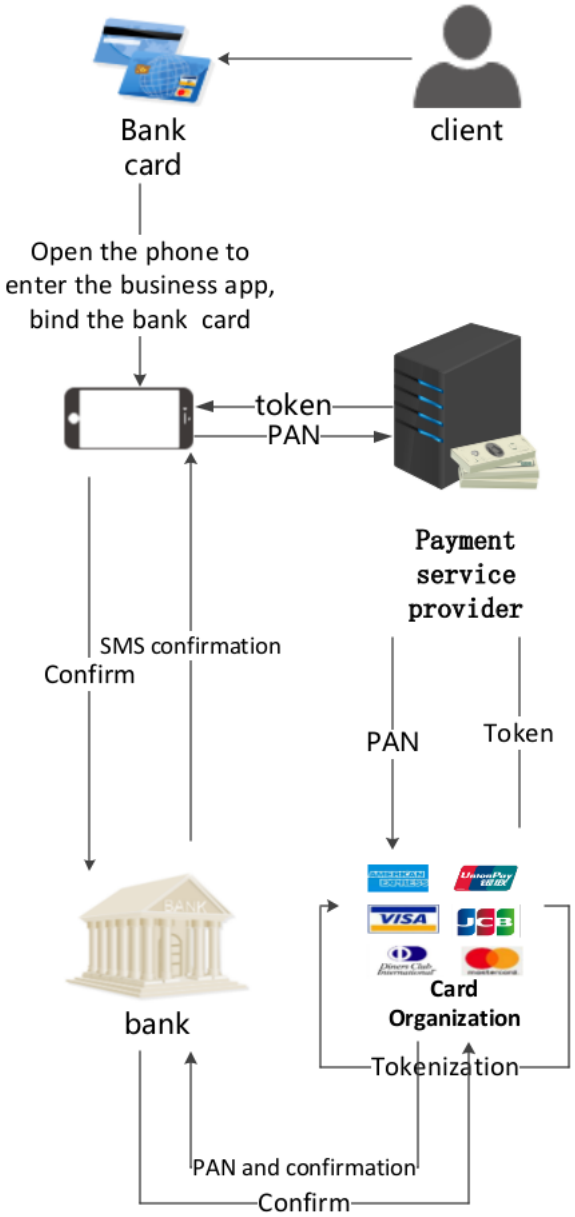

Fig. 3. Token application process.

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. At the same time, it has to be detected by the luhn algorithm, In addition, it is important to distinguish the token from the PAN to token and the PAN issuer easily. Finally, it also needs convenient to distinguish the card issuer of the PAN corresponding to the token.

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 solutions, which requst the token corresponding to the provided PAN from a common central database, as described above. 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.

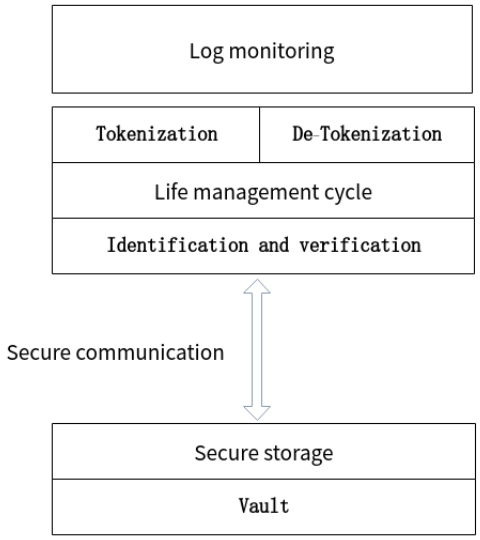

Fig. 4. tokenization service provider of centralized tokenization scheme

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

B. Distributed tokenization technologies

Although traditional centralized tokenization has been widely used, it has also been exposed some critical problems[19]:

• Complexity and cost: Managing large, replicated token databases is difficult and costly, and these databases themselves increase PCI audit scope.

• Integrity: In accurate analytics and other application correlation due to credit card numbers sometimes being replaced by more than one token (a side effect of having a distributed token database).

• Security and risk: Approaches without independent and reviewable security proofs increase breach risk and do not meet QSA(Quality Security Assessor) evidence requirements, and thus cannot achieve PCI compliance. In the event of a breach that leaks cardholder details, merchants using such approaches have no grounds to avoid significant penalties.

• Performance and scale: Tokenization performance is slow and very difficult to scale.

PCI use case completeness: Tokenization is not suited to offline environments, such as web browsers or card swipe terminals. Supplementary solutions are required for PCI DSS audit scope reduction in such applications.

In response to these problems, many companies have proposed distributed tokenization schemes one after another. The main feature is that the generation of tokenization is not concentrated in one server, but can be distributed in various places. Each place can generate the same unique token.

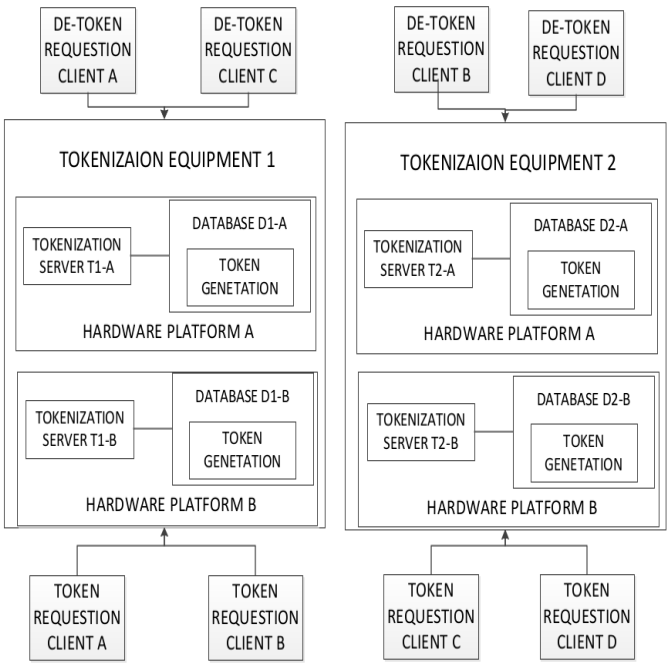

Fig. 5. Distributed Tokenization Scheme of MICRO FOCUS

Figure 4 shows the distributed tokenization scheme of MICRO FOCUS[20]. Tokenization equipment can be used for tokenziation and de-tokenization. And it can have multiple and distributed in different geographical locations. User A may exchange tokens for PAN in tokenization equipment A, and may request de-tokenization operations in tokenization equipment B, and vice versa. In this way, there can be no data center dedicated to manage tokenization and de-tokenization, but can operate on any tokenization equipment.

The token generation process of mainstream distributed tokenization scheme consists of the following features:

• Pre-positioning the same lookup tables to each tokenization equipment. Lookup table of MICRO FOCUS schem[20] as shown in table 1.

• Using lookup tables to design mapping schemes, often using iterative mapping, rotation, etc.

• Don't store the mapping relationship between PAN and token.

The distributed solution relieves some problems of the centralized system to some extent. In particular, the elimination

of centralized data centers can greatly reduce costs. However, new issues have also been traced. Once the lookup table leaks, it will have a major impact on the security of the entire solution. Moreover, the lookup table is the same in all local devices. On the other hand, it is not very convenient to withdraw tokens.

Table 1 Lookup Table.

TOKEN	SENSITIVE NUMBER
4876 9865	2348 9286
7374 2625	2827 6438
...	...
...	...
...	...

C. The process of binding bank card.

Tokenization is a key link for binding a bank card to a mobile phone, but the security of the entire process also requires the application of multiple technologies. Since distributed tokenization are not widely used, the following are discussed in centralized tokens.

In the entire process, apart from the customer himself, two departments have played a major role:

1) TSP(Token Service Provider): The TSP is mainly responsible for the Token management related work in the Tokenization system, and maintains a series of components related to Token operations. The TSP provides the services provided by these components in the form of APIs for other roles to call, mainly including the following aspects: .

1) Tokenization component;

2) De-Tokenization component;

3) ID&V components:During the Token generation process, the user's account number needs to be verified to assign different guarantee levels to the Token. Different guarantee levels limit the range that the Token can use. This verification is performed by the ID&V component. ID&V actually accepts sensitive information from a group of users and outputs the user's Token security level after a certain algorithm;

4) Token Lifecycle Management Components;

5) Token and Card Data Vault:The Token vault is the core of data storage in the TSP. In addition to the mapping between the user Token and the PAN, it also stores the sensitive information that the user uses for the ID&V process. There is no such thing in the distributed tokenization scheme.

TSP is mainly undertaken by card organizations, banks, or some large financial companies.

2) TR(Token Requestor): TR is mainly responsible for two aspects of work in this payment system.

On the one hand, TR needs to provide a set of APIs for developers of electronic wallets. The API includes two parts:

1) The first part of the API provides cardholder lifecycle management, such as user registration, user login, and user revocation.

2) The second part is the interface related to the Token service, including the application, update, unbundling, and loss reporting of the Token.

On the other hand, when the TR receives the Token application request of the user, it needs to call the corresponding API of the TSP to route the request to the corresponding TSP, and then the TSP returns the value of the Token and some other related data and finally forwards it to the user.

In today's market, TR is mainly played by payment service providers. TR first needs to register with the TSP. The registration process and the data involved may differ according to different TSPs. After the registration is completed, TSP assigns a unique ID (Token Requestor ID) to the TR for the TSP to identify the legitimacy of the TR. Each TR ID corresponds to a TSP, so a TR can have multiple TR IDs. After the TR can apply for the Token, the specific way to call the API interface provided by the TSP.

Figure 1 shows the mainstream process of binding bank cards to mobile phones today:

1,Open the payment software app and start binding the bank card and enter PAN;

2,The phone sends the PAN over the encrypted channel to the server of the payment service provider,

3,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.

4,The card company confirms with the card issuing bank of the PAN, and then the card issuing bank sends a random code to the user's mobile phone through the short message, allowing the user to enter the random code on the mobile phone for confirmation.

5,After the user confirms, the issuing bank will reply with confirmation information to the card organization. The card organization uses the TSP to generate a token reply to the payment service provider, which then stores the token on the server and responds to the user's mobile phone.

6,Finally bind tokens to mobile terminals instead of PAN for mobile payment transactions

Figure 3 shows the payment system framework of China UnionPay. Its entire bank card binding process is basically the same as described above. However, during this process, if the payment service provider maliciously saves the PAN, it is difficult to deal with it.

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. As shown in Figure 5:

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

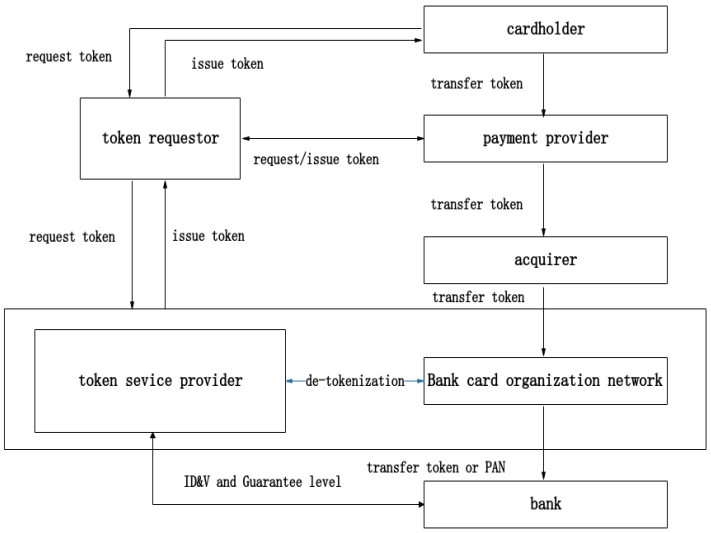

Fig. 6. China UnionPay payment tokenization system framework

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.

The PAN leak is really avoided in Alibaba's solution.

The tokenization technology and bank card binding scheme are the bottom layer of mobile payment technology. The former centralized solution needs to solve the problem of large-scale data storage and a single token generation location, and the distributed solution needs to solve the problem of the leakage of the lookup table. The latter needs to solve the problem of PAN being hijacked by a third party during the binding process.

IV. Mobile Terminal Security

After the mobile phone binds the token, it begins to act as a mobile payment terminal. The mobile terminal need often authenticates the payment and also stores a lot of sensitive information, such as the PIN code of the payment APP,fingerprint and the token. Once the mobile payment terminal is invaded by an adversary, the customer will suffer heavy losses. Therefore, the security of mobile terminals is also increasingly concerned by major mobile phone manufacturers and payment service providers.

TEE and eSE are the two key technologies for the security of mobile terminals in mobile payment today.

A. TrustZone

In 2006, the open mobile terminal platform organization OMTP (Open Mobile Terminal Platform) took the lead in

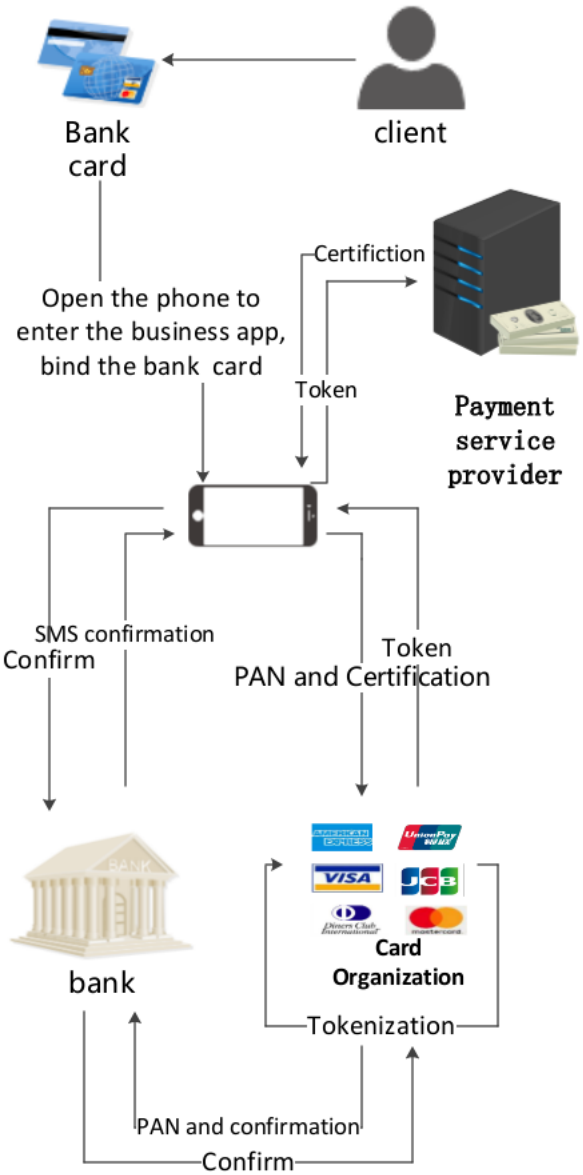

Fig. 7. Token binding process.

presenting a dual system solution: that is, in addition to a multimedia operating system, providing an isolated security operating system under the same intelligent terminal. Isolated security operating systems on isolated hardware are used to specifically process sensitive information to ensure information security. This program is the predecessor of TEE.

Based on the OMTP solution, ARM (the world's largest solution provider of embedded processors whose architectures account for approximately 95% of the mobile phone market) proposed a hardware virtualization technology TrustZone and related hardware in 2006. Implement the plan. TrustZone is a product that supports TEE technology. TrustZone is the basic function of all Cortex-A processors.

TrustZone conceptually divides SoC hardware and software resources into Secure World and Normal World. All operations that require confidentiality are performed in the secure world (such as fingerprint identification, password processing, data

encryption and decryption, and security certification, etc.) The rest of the operations are performed in a non-secure world (such as user operating systems, various applications, etc.), the security world and the non-secure world are converted by a mode named Monitor Mode.

On the processor architecture, TrustZone virtualizes each physical core into two cores, a non-secure core (NS Core), which runs a non-secure world, and another secure core (Secure Core), which run the safe world code.

The two virtual cores operate in a time-sliced manner, occupy physical cores in real time as needed, and switch between the secure world and the non-secure world through Monitor Mode, similar to a multi-application environment under the same CPU, but different from multiple applications. In the program environment, the operating system implements interprocess switching, while the Monitor Mode under Trustzone implements switching between two operating systems on the same CPU.

For more details, please refer to the TrustZone white paper [15].

B. TEE

ARM later provided its TrustZone API to GlobalPlatform, which has evolved into a TEE client API. It is introduced through the ARM architecture security extension, and ARM has become one of the leaders of TEE technology.

GlobalPlatform (the world's leading organization for smart card multi-application management specification, abbreviated as GP) is an international standard organization led by Visa, MasterCard, and other international bank card organizations. Since 2011, it has drafted and developed related TEE specification standards, and has joined several companies. (ARM, etc.) jointly develop a trusted operating system based on the GP TEE standard. Therefore, most of today's Trust OS based on TEE technology has followed the standard specification of GP.

The Trusted Execution Environment (TEE) is a concept proposed by the Global Platform (GP). For the open environment of mobile devices, security issues are also getting more and more attention, not only terminal users, but also service providers, mobile operators, and chip vendors. TEE is an operating environment coexisting with Rich OS on the device and provides security services to Rich OS. It has its own execution space, which is higher than Rich OS's security level, but lower than the security element (SE, usually a smart card). However, TEE can meet the security needs of most applications. From a cost perspective, TEE provides a balance between security and cost.

Among them, the software and hardware resources that TEE can access are separated from Rich OS. TEE provides a secure execution environment for authorized security software (**trusted applications, TA**) while also protecting the confidentiality, integrity, and access rights of TA's resources and data. To ensure the trusted root of the TEE itself, the TEE is authenticated and isolated from the Rich OS during the secure boot process. In TEE, each TA is independent of each other and cannot be accessed without authorization.

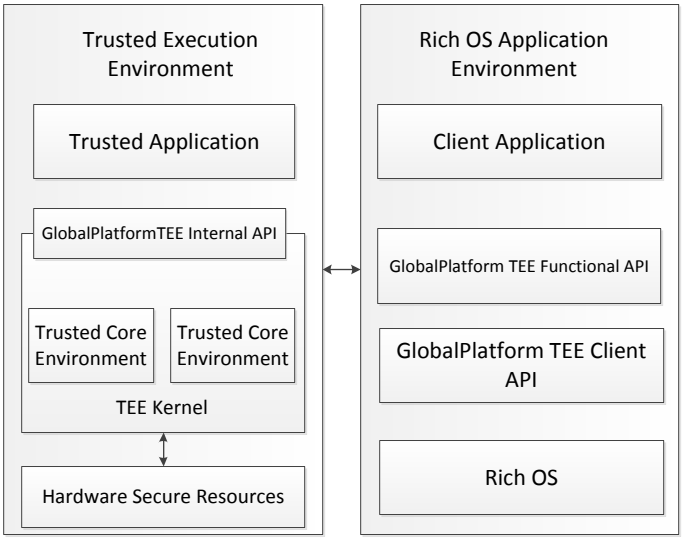

Fig. 8. TEE and Rich Os

GP has made great efforts in the standardization of TEE. The basic specifications include TEE internal API, TEE client API, and of course, there are a series of additional functional API specifications, as well as application management, debugging functions, security protection profile, etc. In development.

The TEE internal API mainly includes APIs such as key management, cryptographic algorithms, secure storage, secure clock resources and services, and an extended trusted UI. Trusted UI means that when key information is displayed and user key data (such as password) is input, hardware resources such as screen display and keyboard are completely controlled and accessed by TEE, and software in Rich OS cannot be accessed. The internal API is the programming interface that TEE provides to TA;

The TEE external API is the underlying communication interface for the client application unning in the Rich OS to access TA services and data.

C. SE

Secure Element (SE) is a platform that can install, personalize and manage applications. It is a combination of hardware, software, interfaces, and protocols that can securely store and use credentials for payment, authentication, and other services. Conceptually, SE can be divided into two areas from the paper [17] :

- Embedded SEs;
- Removable SEs;

1) Embedded SE: The embedded SE is a chip that is integrated into a mobile phone and cannot be removed. According

to research [18], the SE provides the same level of security as smart cards support. The chip is embedded in the handset during the manufacturing process and must be personalized after the device is delivered to the end user [18]

The eSE is the most secure device in mobile phones and often stores fingerprint data with the highest security level, authentication keys, and bank card related information. High-end mobile phones often equipped with fingerprint recognition will be equipped with eSE. For example, iphone 7/8, Samsung s9, Huawei mate 10, etc.

2) Removable SEs: The rSE is a chip that can be removed and replaced in mobile phones. Usually embedded in some replaceable phone hardware , such as SD card, SIM card

SMC: The Secure Memory Card (SMC) provides the same advanced security as a smart card and meets most of the smart card's major standards and interfaces (eg, GlobalPlatform, ISO/IEC 7816, JavaCard, etc.). As described in [18], SMC can host a large number of applications with mobility and large memory.

This year, SMC has slowly withdrawn from the market because major mobile phone manufacturers are no longer supporting SD cards.

UICC: Cards used in existing mobile phones such as SIM, USIM, UIM, etc. are collectively referred to as UICC(Universal Integrated Circuit Card.)

UICC is a general multi-application platform for implementing smart card applications of SIM or USIM. UICC provides an ideal environment for personal, secure, portable and easily remotely managed NFC applications via OTA technology. It can host non-telecom applications from various service providers such as loyalty, ticketing, healthcare, access control and ID applications. GlobalPlatform provides the most promising standard for UICC life cycle management (or card content management)[17].

D. comparision

The TEE is running in the device and provides a framework for security between ordinary RichOS and SE (smart card). Many current security architectures are based on Rich OS + SE. In fact, this cannot provide a "just good" fit in terms of convenience and cost. Because some small payments, DRM, corporate VPN, etc., the required security protection is not high, does not need a separate SE to protect, but it can not be directly in Rich OS, because of the latter's openness Make it easy to be attacked. So for such applications, TEE provides the appropriate protection strength and balances cost and ease of development.

For attack resistance, SE is the highest and Rich OS is low. For access control, it is similar to anti-attack, but Rich OS can do more; for the user interface, SE is powerless, and Rich OS is the most abundant; development is easy. On the other hand, the Rich OS is the easiest. Of course, if the TEE standard is done well, it can be done quite "easy". On the processing speed, TEE and Rich OS are equivalent. Because the same physical processor used by both, SE is certainly slow; Finally, the SE is physically removable.

After joining TEE, the extra cost increase is very low, and it can reach a medium protection level; if you want to achieve high-level protection, you will need additional costs. The analysis of this figure does not mean that the appearance of TEE makes the device not need SE, but as a medium security level, to meet the corresponding security objectives.

Table 1 Comparison.

	REE	TEE	SE
	Only software	Software and HW	Software and Tamper resistant HW
Cost	No extra cost	Low extra cost	High extra cost
Attack Resistance	Weak	General	Strong
Access Control	Weak	General	Strong
User Interface	Abundant	Can do a little	Powerless
Ease of Development	Easy	Easy with right Standard	Hard
Processing Speed	Fast	Fast	Slow

With the support of major chip manufacturers, mobile phones using ARM architecture chips now include Trustzone technology. The gap between the real high-end phones and low-end phones is on eSE. In addition to PIN payment authentication, fingerprints are supported by high-end handsets of major mobile phone manufacturers. iphone X now supports face recognition. It is very necessary to store these sensitive information in eSE.

V. PAYMENT COMMUNICATION SECURITY TECHNOLOGIES

After obtaining a secure payment mobile terminal, how to ensure payment communication security has become a hot topic in this field.

Payment communication technology is intuitively experienced by customers. In the customer's eyes is how to pay the money to the recipient. So people often use it to name payment. For example, Alipay, WeChat, etc. are called QR code payment. While Apple, Samsung, etc. are often called NFC payments. In fact, the former only uses a two-dimensional code to transfer one-time payment passwords. What really pays for the payment is the one-time payment password. Whatever the method, as long as you can transfer the one-time payment password, you can conduct a payments, another way such as audio. The latter's NFC is actually an interactive near-field communication.

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?

1) QR code working principle: The QR code itself cannot make payment authorization, since the actual payment authorization is the one-time payment password which encoded in the QR code. The one-time payment password is a series of digits(which we calld **payment password**shows on Fig 10). 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 one-time payment password will be told in section 6.

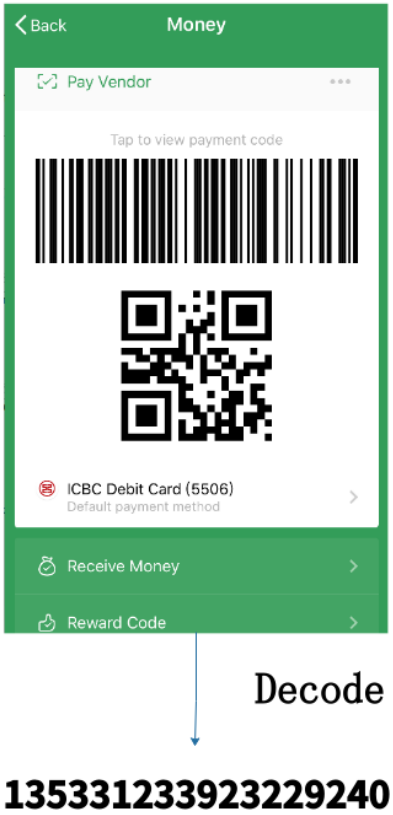

Fig. 9. Qne-time payment password

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 cod 49(shows at Fig 7) and PDF 417(shows at Fig 8):

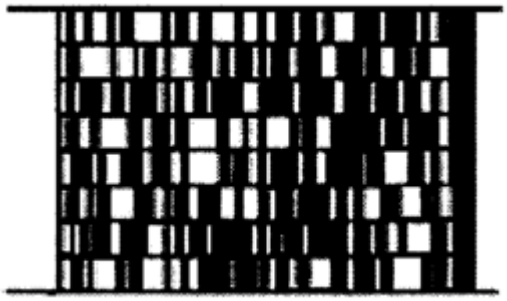

Fig. 10. code 49

Fig. 11. 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)

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.

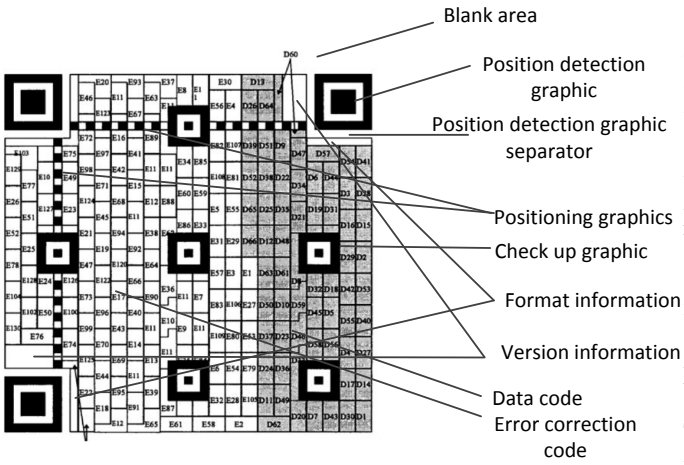

Fig. 12. The structure of the QR code

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

2) QR code payment security analysis: QR code is only for data transmission, and its security is based entirely on one-time passwords.

1,Eavesdropping : QR code is very easy to be eavesdropped, such as implanting a Trojan on a mobile phone, or placing a miniature camera on a PoS machine.

2,Data Modification The QR code itself is encoded and decoded by a fixed standard, so it is easy to tamper with after its own generation. However, one-time payment passwords cannot be easily tampered with without knowing algorithms and keys. So QR code payment can resist data modification

3,Man in the middle Attack: QR code can only be transmitted in one direction. There is no man-in-the-middle attack.

4,Lost devices: Anyone who finds a lost device can use it just like a lost credit card. In this case, manual security in mobile devices is the only solution, such as secure access to the phone via some PIN code or personal identification number.

B. 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) Audio working principle: 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. 13. A complete sound packet.

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

The security analysisof Audio payment is almost the same as QR code.

C. NFC

NFC is a technology that mobile phone manufacturers strongly recommend in the field of payment communications. Many new mobile phones released by Apple, Samsung, Google, Xiaomi, Huawei, etc. all support NFC.

Near Field Communication (NFC) is a wireless technology that can communicate within a short distance of four to ten centimeters. It is based on radio frequency identificatio (RFID) technology. For communication, NFC devices genera radio frequencies in the 13.56 MHz spectrum. If the receiver close, data can be received by the magnetic inductive couplir principle. Transmitters and receivers are small chipsets th can be embedded in handsets, POS (Point of Sale) terminal cards, and other devices.

The NFC Forum was established in 2004 to standardiz NFC technology. It defines NFC as: NFC is a short-range wir less connection technology (also known as ISO 18092) th provides intuitive, simple and secure communication betwe electronic devices. The NFC operating frequency is 13.5 MHz and the communication distance is limited, supportir data rates of 106 Kbps, 212 Kbps, and 424 Kbps. Therefor NFC is suitable for transmitting short messages or messages in short time intervals.

NFC not only improves security and data transmission efficiency, but also has interactivity. More importantly, NFC is compatible with existing popular technologies (such as RFID, smart card contactless cards). This means that existing shops and systems do not need to replace their infrastructure to support NFC.

NFC technology is a key technology for mobile phone manufacturers to enter mobile payment. On the surface, the mobile payment market today is mainly the QR code battle NFC. Therefore, it is very important to evaluate the performance of NFC technology and its location.

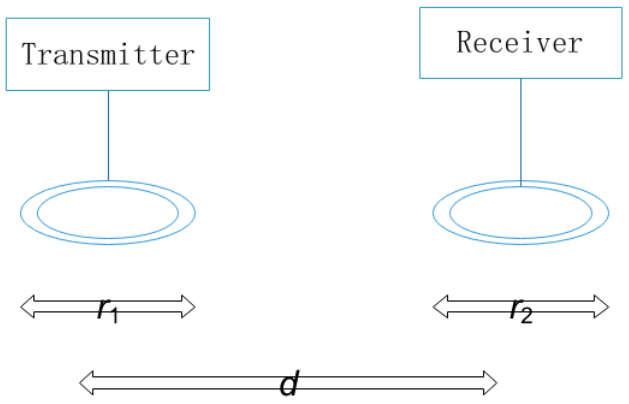

Fig. 14. Inductively coupled near-field system.

NFC devices communicate through magnetic induction signals. Therefore, during transmission, energy is coupled between the transceivers, rather than electromagnetic radiation as in traditional wireless communications. Magnetic induction is discussed in detail in [37-38]. Magnetic induction theory and its application in NFC are also discussed. Figure 10 shows a short range inductively coupled NFC antenna, usually in centimeters. In close proximity, information can be exchanged between these transceivers via magnetic induction. The equivalent circuit diagram of these antennas is shown in Figure 11. The power mathematical derivation at the receiver of a given circuit is derived in [37], where the power of the receiver can be expressed as:

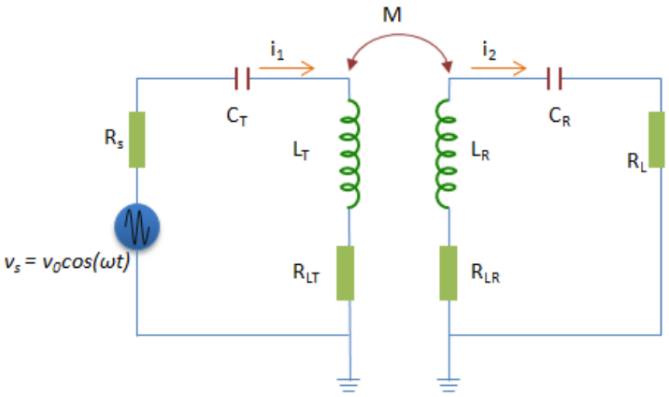

Fig. 15. The equivalent circuit of a pair of antennas.

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

where:

P_T :Transmission power;

$\eta_T = R_S/(R_S + R_{LT}), \eta_R = R_L/(R_L + R_{LR})$:Efficiency of transmitter and receiver antenna:

$Q_T = \omega_0 L_T/(R_{LT} + R_S), Q_R = \omega_0 L_R/(R_{LR} + R_L)$: Quality factors of transmitter and receiver antenna,;

r_T, r_R : Radius of transmitter and receiver;

μ_0 : Permeability of air (=1);

μ_T, μ_R :Relative permeability of transmitter and receiver antenna coil core ;

d :Distance between receiver and transmitter antenna.

NFC communication involves three types of NFC devices: smart phones, NFC tags, and NFC readers. The possible interaction styles between NFC devices provide three different modes of operation, as shown in Figure 14,15,16: Card reader/writer mode, peer-to-peer mode and card emulation operations mode [39-40].

1) NFC tag: NFC tags are usually embedded in items (which can be read from them),such as POS, electronic devices, etc. It is a small chip that is usually hidden on a sticker with an NFC logo in order to make the user aware of its presence. These tags often contain small data with valuable information based on their application.

2) NFC smartphone: NFC smartphone is the mobile phone that can use the NFC communication function, which is typically composed of various integrated circuits such as the NFC communication module. The NFC communication module is composed of:

- NFC Contactless Front-end (NFC CLF);
- NFC antenna;
- an integrated chipset referred to as an NFC Controller (NFCC):manage the emission and reception of the signals;
- modulation/demodulation.

The SE(mentioned in the section 3)of NFC technology enables secure storage and secured transactions among NFC smartphone [18]. Currently, the promising SE alternatives for NFC transactions are eSE, SIM-based SE(rSE), and Host Card Emulation (HCE). For the eSE option, the NFC Controller is connected to the SE through either Single Wire Protocol (SWP) [41] or NFC Wired Interface [42]. SWP is the most commonly used protocol between the NFC interface and the SE. It can be used for all SE-form factors and provides optimal interoperability with multiple protocols [43].

The device that starts communications is called the initiator, and the responder is called the target. NFC smartphones and NFC readers use their own power supply and therefore are active devices, while NFC tags use the other party's power supply and are therefore called passive devices. All initiator devices are usually active devices, but the target device can be active or passive, depending on the mode of operation.

3) NFC operate model:

a) Read/Write mode: In reader/writer operating mode, a smartphone initiates the communication as an active device. NFC has a predefined data format called NDEF data format. When the NFC phone is in read/write mode, it can read or write data to a supported tag type. Fig 14 shows the

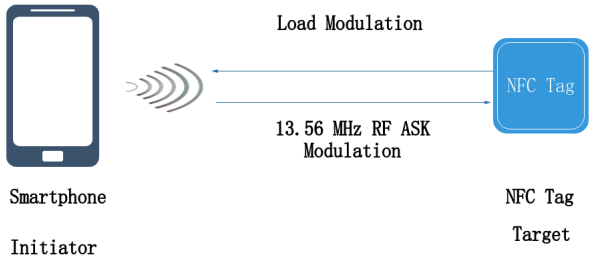

Fig. 16. Reader/Writer mode.

b) Peer-to-Peer mode:

In peer-to-peer mode, two smartphones establish a two-way connection to exchange data. In this mode, two NFC phones can exchange data when they are close. For example, two business partners can exchange their personal information with each other by bringing their NFC-enabled phones close to each other. Another popular use is to switch connections to other standard technologies; NFC connections can be used to set-up Bluetooth pairing or Wi-Fi setup. After successful setup, the phone can use Bluetooth or Wi-Fi connection.

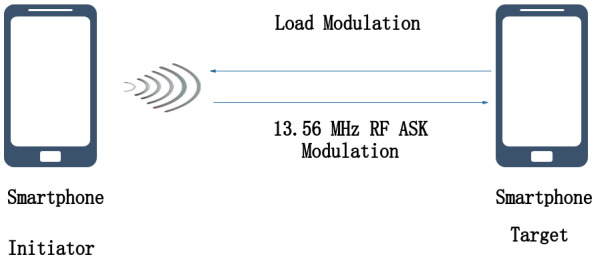

Fig. 17. Peer to Peer mode.

c) Card Emulation Mode:

An NFC smartphone can acts as a NFC tag or a kind of contactless card in card emulation mode. The NFC reader interacts with the SE directly. When it act as a tags, it can be read by existing traditional card readers. For an instance, it can be used as an identity card or bus card in dally life. Also, most common usage would be to emulate credit cards or points cards which can be used at POS terminals for payments. Fig 16 shows card emulation mode.

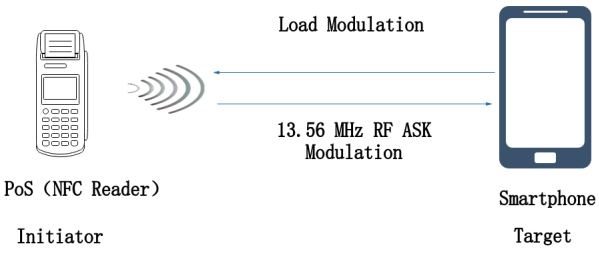

Fig. 18. Card Emulation Mode.

The RF layer of NFC communication is based on the ISO/IEC 14443 contactless smart card and the JIS X 6319-4 Felica standard[45]. It uses digital protocols and analog technologies similar to smart cards and is fully compatible with smart card standards based on ISO / IEC 14443 Type A, Type B and Felica[44]. In addition, it also uses the NFC Forum's analog, digital protocol and physical layer activity specifications[46]. Fig 17 shouws the Protocol stack of card emulation operating mode.

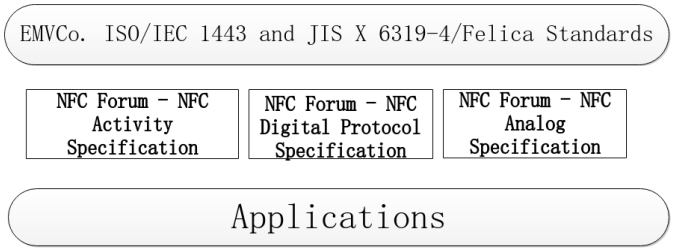

Fig. 19. Protocol stack of card emulation operating mode.

4) NFC payment security analysis: 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 : In active mode, NFC does not provide a defense mechanism against eavesdropping. By eavesdropping, the attacker can use a suitable antenna to receive the transmitted information, but this antenna should be close enough. However, in [8] it was discussed that eavesdropping in NFC is difficult if the device is operating in passive mode.

2,Data Modification Attackers may use different RF fields to tamper with data. However, 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 that they can check the RF field generated by the attacker to avoid conflicts.

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.

4,Lost devices: Manual security in mobile devices is the only solution. 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.

Through the introduction of NFC we know that NFC has high security but the hardware requirements are much higher than QR code and Audio. And need to be compatible with a variety of protocols. What is even more inconvenient is that many PoS machines in shopping malls (especially in some less developed areas) do not become NFC readers and do not support NFC. These have become obstacles to the promotion of NFC.

D. MST

In order to solve the compatibility problem of the old magnetic stripe cards mentioned in the last subsection, Samsung also uses MST technology in addition to NFC technology on its own mobile phones.

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 compare to Apple Pay and Android pay is support for magnetic stripe card payments.

1) MST working principle: 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. With the help of tokenization technology, MST is not afraid of being copied like a traditional magnetic stripe card. At the same time, its compatibility with today's PoS devices is also higher than NFC.

Figure 18 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(Figure 19).

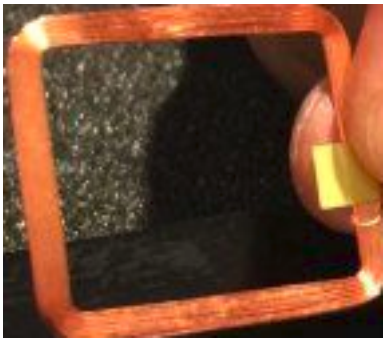

Fig. 20. token service provider

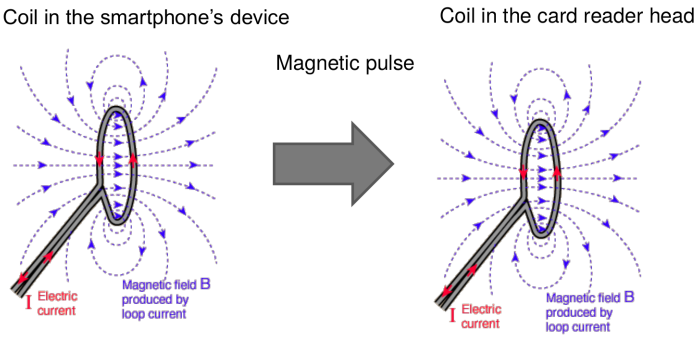

Fig. 21. Emitting magnetic pulse.

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.

2) MST payment security analysis: In fact, the principle of MST is to emit a magnetic field. However, payment security cannot be solved by a copper coil. The simple principle of

electro-magnetism is only the basic theory of this technology. 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.

1,Eavesdropping : MST does not provide a defense mechanism against eavesdropping. In [46], the authors found that using a small packet-sized loop antenna can effectively collect signals at a distance of at least 2 meters from the signal source. Therefore, eavesdropping attacks are effective for MST.

2,Data Modification: The MST information obtained by eavesdropping can be decoded by the method shown in [46], but it is difficult to obtain the information obtained after tampering. For example, add a signature after the information.

3,Man in the middle Attack: MST code can only be transmitted in one direction. There is no man-in-the-middle attack.

4,Lost devices: The same as NFC.

Although MST has greatly improved its compatibility, its security has been greatly reduced. The MST payment can be considered in some situations where the security requirement is not high or only the magnetic stripe card is supported. It can be seen that for Samsung, MST payment is only a supplement to NFC payment.

E. comparision

QR code and Audio have high hardware compatibility. Even a very cheap mobile phone also can supports this payment method, and the cost is very low. This may be an important reason for it large-scale promotion in China. Because of its inability to defend against eavesdropping attacks, its security is a big problem. NFC is just the opposite. Under the premise of terminal security, Samsung's MST payment security is similar to that of QR code, but it requires the moderate cost and hardware.

Table 2 .

	QR code	Audio	NFC	MST
Cost of device	Low	Low	High	Moderate
Auth and Encry	No	No	Yes	No
Data Transmission Direction	One-way	One-way	Two-way	One-way
Hardware compatibility	High	High	Low	Low
Eavesdropping Attack	effective	effective	ineffective	effective
Data Modification	ineffective	ineffective	ineffective	ineffective
Man in the middle Attack	*	*	ineffective	*
Loss of device protection	Rely on terminal security	Rely on terminal security	Rely on terminal security	Rely on terminal security

VI. ONLINE PAYMENT

This section and the next section mainly describe the payment technology of payment service providers. Payment service providers mainly refer to Alibaba, Tencent, paypal and others. Their mobile payment technology is mainly divided into network transfer payment and offline payment.

Network 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. Network transfer payment process

The customer can obtain a URL by scanning the QR code, etc., and pay the store through the specific website address. This approach is more like a mobilization of previous web page payments. After the server receives the payment information, there are two situations:

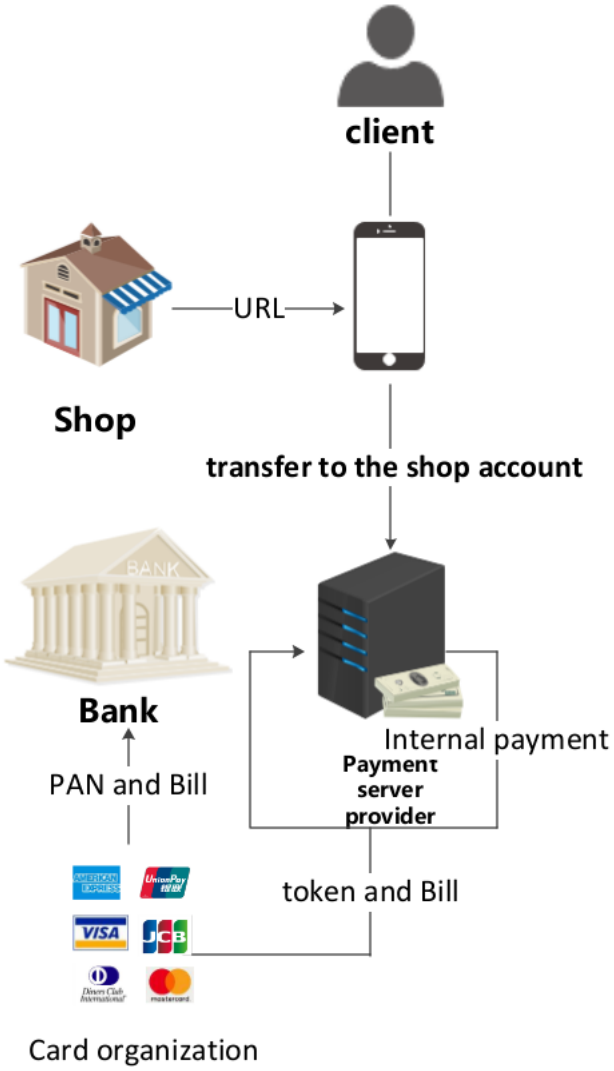

Fig. 22. Online payment.

Pay with your account balance: In this way, the payment service provider does not need to interact with the bank, but can only perform settlement within the server.

Pay with your bank card: The payment service provider will give the card corresponding tokens , bills and other information to the card organization. The latter continues to interact with the issuing bank and complete the payment. t should be noted that the transaction is actually completed by the issuing bank paying money to the payment service provider's account on the bank's account, and then the payment service provider adds the corresponding balance to the customer's account on the server of the customer.

B. 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.

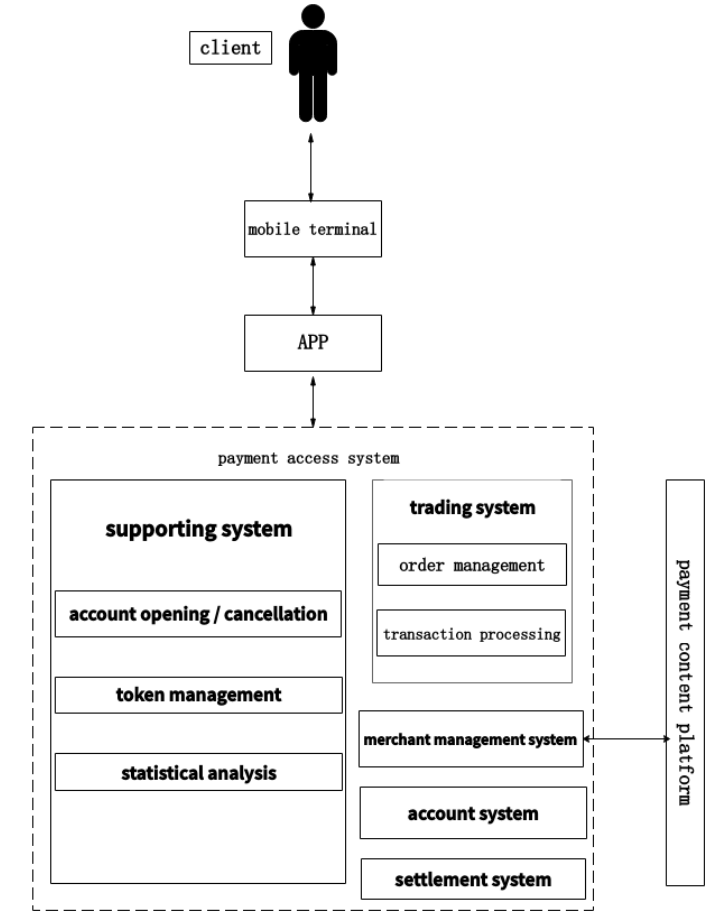

Fig. 23. Network payment system.

C. Through email

VII. 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. 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.

It mainly binds the bank card to the account of the corresponding payment provider and uses the TOTP technology to generate the payment password to pay. Figure 22 shows the entire process of offline payment from client to bank, including TOTP payment represented by Alipay and Wechat.

As the Fig 22 shows, after the TOTP is generated by the mobile phone, QR code or audio is used as a medium to pass TOTP to the shop. The shop transmits the TOTP and payment information to the server of the payment service provider through which decodes the TOTP and certification. If certified, the subsequent process is exactly the same as online payment.

A. One-time password payment system

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 generates the OTP using the token, ID and the TOTP algorithm. The payment service provider server uses the same token, ID and decryption algorithm to verify the OTP.

B. 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(Fig 7). This 18-digit number is the one-time password.

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

$$HMAC(K,m) = H((K' \; xor \; opad)||H((K' \; xor \; ipad)||m))$$

- H:hash function;
- 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);

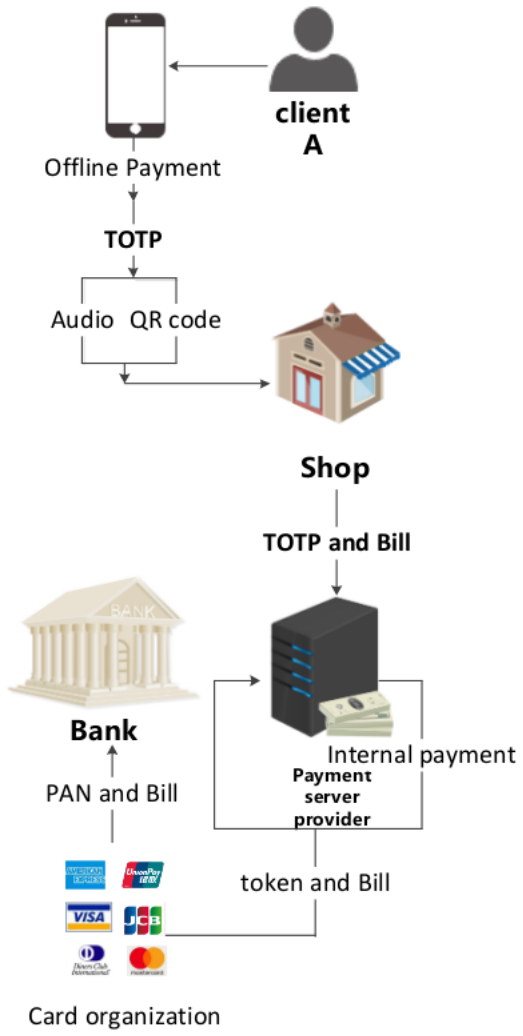

Fig. 24. Offline payment.

• 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:

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

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

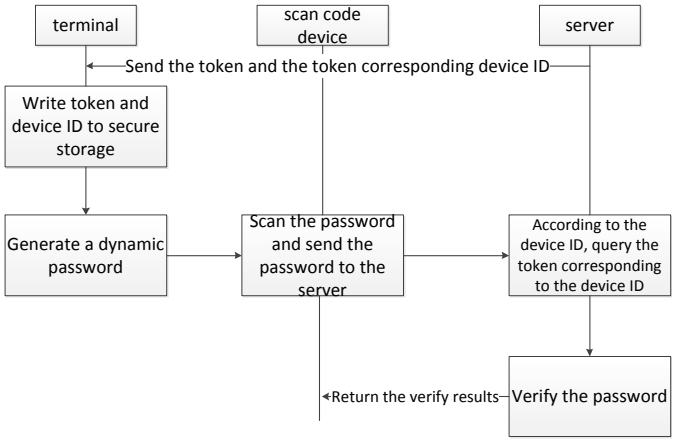

Fig. 25. Time-Based One-Time Password.

• T0:The time step to start the calculation;
• TS:Time Step.

Figure 23 is a TOTP generation algorithm that Alipay used.
The terminal calculates the dynamic password by using the pre-stored token and the current time as input values of the first preset algorithm.
The first preset algorithm may be an arbitrarily formed irreversible algorithm
1, time synchronization algorithm (TOTP);
2, event synchronization algorithm (HOTP);
3, challenge response algorithm (OCRA);

The first information can be any of the following:
1, dynamic password: a sequence of random numbers.
2, the combination of dynamic password and current time value: such as: 765645 (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

The authentication algorithm is as follows:
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

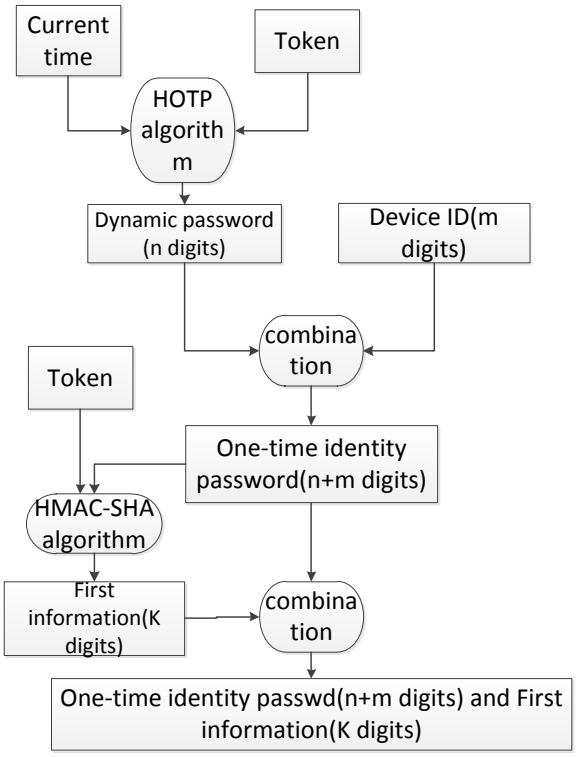

Fig. 26. Time-Based One-Time Password.

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

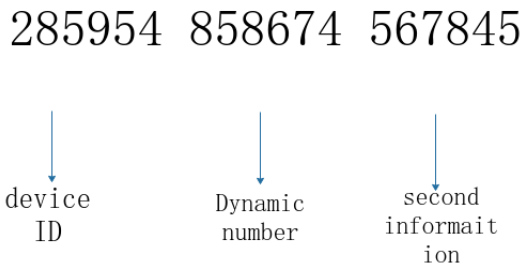

Fig. 27. Offline payment.

The latest TOTP algorithm of Alipay and WeChat is different from this, but the basic ideas and methods are similar.

VIII. Mobile phone emulate IC card

Mobile phone manufacturers technology in mobile payment is mainly embodied in the combination of hardware and software. Samsungs KNOX and eSE, Apples co-processor, and Googles HCE technology allow users bank cards to be securely bound to their phones.

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 companies have taken a different path from companies such as Alibaba and Tencent when they entered the payment industry.

Different from the use of the two-dimensional code, audio, and other means. They work directly with banks and are committed to using mobile phones to simulate IC card payments which hope to have a swipe experience on the mobile phone.

A. bank card

At the beginning, we briefly introduced the 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.

B. Sumsung pay

In order to be able to simulate the bank card payment as much as possible, Samsung used two sets of payment plans, which are the aforementioned NFC and solutions.

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.

In order to improve the security of mobile phones, Samsung developed KNOX in terms of software. KNOX is a solution that guarantees end-to-end security. It provides defensive-grade security protection from hardware to application layer. KNOX integrates the Android System Security Enhancement Kit (SE Android) developed by the National Security Agency of the United States and applications. Hardware and Android Framework integrity management services. At the application layer, KNOX provides a ”container” solution that isolates the mobile device from its office use and personal use.

Samsung uses security combination of eSE and trustzone in terms of hardware. In terms of hardware, Samsung uses the security combination of eSE and trustzone. Sensitive data such as PINs, tokens, fingerprint etc. are stored in the eSE, and payment operations are performed under the TEE.

C. Google pay

On February 20, 2018, Google announced that it has integrated Android Pay and Google Wallet, officially launched a new payment service Google Pay

1) Android Pay: Android Pay is a mobile payment service launched by Google in 2015. It is based on the foundation of Google’s electronic money package. It allows users to store credit or financial cards in mobile phones and use Near Field Communication (NFC) to transmit them. Card information to complete the payment process to replace the past credit card payment methods, while the original Google e-money packs still exist, mainly supporting network-based Play Store shopping and some application-based point-to-point payments.

The hardware limitation of using Android Pay is not severe. As long as the system is Android 4.4 or higher, and the built-in NFC chip, Android Pay can be used. In other words, as long as this condition is met, not only the mobile phone, but also the Android tablet can With Android Pay.

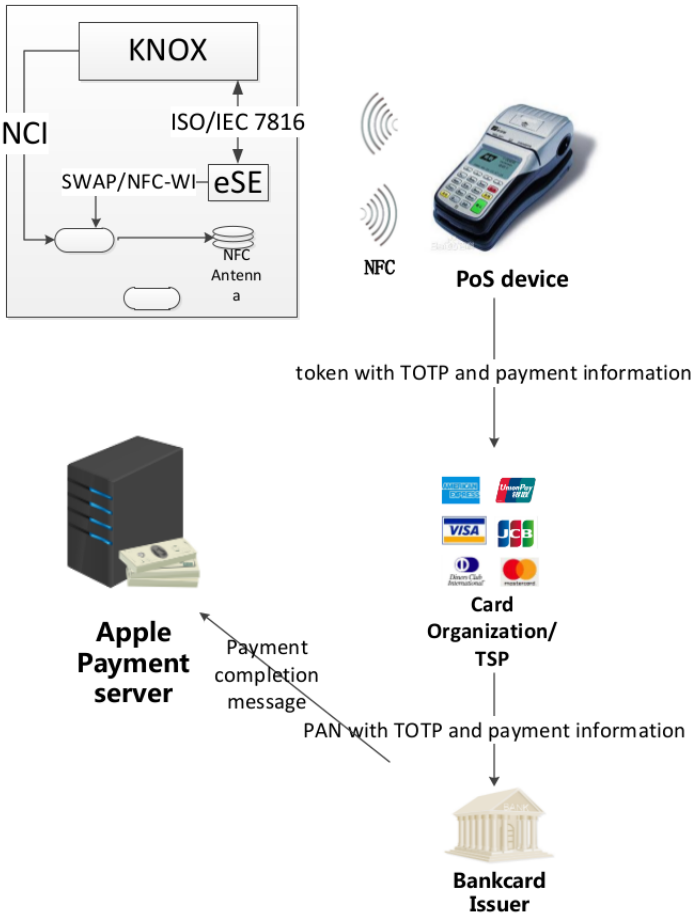

Fig. 28. Samsung payment.

NFC technology has been around for more than a decade and has been called promising mobile payment technology for the past few years. But even today, NFC-enabled mobile phones are increasingly becoming the standard for smartphones, and NFC-based mobile payments have not formed widespread acceptance among consumers. One important reason is that everyone is rushing to control the Secure Element of NFC technology. The security element, as the name implies, is to ensure the security of property information. Controlling this can control the cost of each transaction. SE has led to endless battles between financial institutions, OEMs and operators. There is no way to unite them, which makes NFC mobile payment development slow.

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

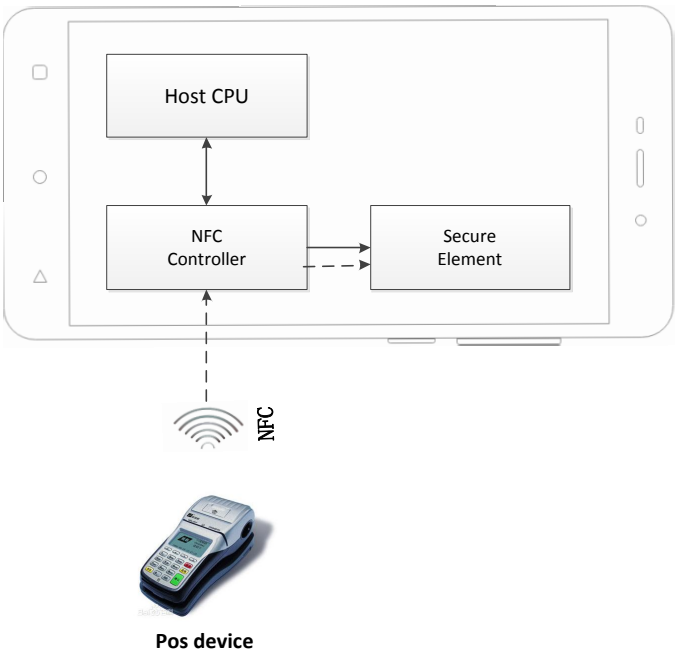

Fig. 29. NFC card emulation with a secure element.

platform.High-risk behaviors such as equipment modification occur, and KNOX can invalidate sensitive data on the device.

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.

2) HCE(host-based card emulation): There are two ways to implement card emulation on an NFC-enabled mobile phone: one is hardware-based, called virtual card mode; the other is software-based, called host card mode (Host Card Mode).

In the virtual card mode, the security module SE (Secured Elemen) needs to be provided. The SE provides secure storage of sensitive information and provides a secure execution environment for transactions. The NFC chip acts as a contactless communication front end, forwards the commands received from the external reader/writer to the SE, and then processes them by the SE and replies via the NFC controller.

In the host card mode, there is no need to provide the SE. Instead, the SE function is performed by an application running in the mobile phone or a server in the cloud. At this time, the data received by the NFC chip is sent by the operating system or the application in the mobile phone, or The interaction is done through the server that the mobile network sends to the cloud. Both methods are characterized by the limitation of the built-in SE of the mobile phone. The beauty of this standard is that it does not require the entire industry to fight in order to control the safety elements.

NFC standard support for Android:

The NFC standard provides support for many smart card communication protocols, and the Android 4.4 system also supports many contactless smart card protocols including mainstream smart card applications. Therefore, using NFC mobile phones and HCE applications, it is possible to easily simulate different types of smart card applications. .

Many NFC reader terminals on the market also support these protocols, including an NFC-enabled Android device as the reader itself. This way we can deploy an end-to-end NFC solution using HCE technology using only Android devices.

The Android 4.4 system uses the ISO-DEP standard protocol developed by the NFC Forum (based on the ISO/IEC 14443-4 (ISO-DEP) standard) for data transmission, and the transmitted data units are called Application Protocol Data Units (APDUs).

In addition, the Android system only requires support for the top-level NFC-A (ISO/IEC 14443-3 Type A) technology in terms of digital protocols (equivalent to the MAC layer protocol), and for the NFC-B technology (ISO/IEC 14443-3 Type B) support is optional, these technologies provide solutions including initialization, collision detection, etc.

The HCE technology on the Android system is implemented through system services (HCE services). One of the great advantages of using the service is that it can always run in the background without requiring a user interface. This feature makes HCE technology ideal for transactions such as loyalty cards, transportation cards, and access control cards. When users use them, they do not need to open the program. They only need to put the phone in the NFC reader's identification range. The transaction will be in the background. get on. Of course, it is more recommended to provide the user with a supporting HCE application UI interface. In addition to using the smart card as an ordinary smart card, the UI interface can also provide users with more online service functions, including inquiries, recharging, and information push.

When the user puts the mobile phone into the recognition range of the NFC reader, the Android system needs to know which HCE service the card reader really wants to interact with, so that it can send the received data to the corresponding HCE application. HCE refers to the ISO7816 specification

and defines a method to select the corresponding application through the application AID. Therefore, if you want to deploy NFC applications for your new card reading facility, you need to define your own AID.

HCE technology to achieve NFC simulation:

To implement NFC card emulation using HCE technology on mobile phones, we must first create an HCE service that handles transaction transactions. Android 4.4 provides a very convenient base class for HCE services. We can implement our own HCE services by inheriting base classes. If we want to develop an existing NFC system, we only need to implement the application layer protocol expected by the NFC reader in the HCE service. On the other hand, if we want to develop our own new NFC system, we need to define our own protocols and APDU sequences. In general, we should ensure that the use of a small number of APDU packets and a small amount of data during data exchange, so that users do not need to spend a lot of time on the phone on the NFC reader.

The HCE technology only implements sending the data of the NFC reader to the HCE service of the operating system or returning the reply data to the NFC reader. However, the processing of the data and the storage of the sensitive information are not specifically implemented, so HCE Technology is the protocol and implementation that simulates NFC and SE communications. However, the HCE does not implement SE, but uses the NFC and the SE to tell the NFC reader that there is SE support behind it, so that the security assurance of the NFC service can be completed in a virtual SE manner. Since there is no SE, what does the HCE use as the SE? The solution is either a simulation of the local software or a simulation of the cloud server. How the SE responsible for security is implemented through localized software or a remote cloud, and can guarantee security, requires HCE vendors to consider and implement their own.

HCE scheme and SE scheme routing and compatibility:

Many Android 4.4 mobile phones that support HCE function also support the SE mode such as SWP-SIM or SWP-SD to implement the mobile payment function. Therefore, there is a problem of applying AID routing, which is usually caused by the AID routing table in the CLF chip. Responsible for the related routing work, the mobile phone manufacturer is responsible for the development of specific rules

Because the routing table of the CLF chip is differentiated and routed through the application AID in the Select command sent by the card reader terminal, the specific smart card applications supported by the HCE applications in the SE (SWP-SIM) and the mobile HOST CPU are each supported. If the AIDs are different, then there will not be any routing and compatibility issues. All applications can be correctly identified and routed to SE (SWP-SIM) or HCE applications, and the transaction can be completed and processed normally.

If SE (SWP-SIM) and the HCE application in the mobile HOST CPU support the same AID in the smart card application, there is a problem of routing priority. At the same time, the device that supports SE (SWP-SIM) is upgraded to Android4. After .4, compatibility issues for legacy applications in SWP-SIM.

According to the requirements of Android API provided by google, HCE APP has a higher route priority. It means that if there is an application with the same AID, it will be preferentially routed to the HCE application for processing. Then the application of the same AID in SWP-SIM will be Can't be called and used, there will be system upgrade to version 4.4, can not be compatible with existing applications, unless the HCE application is not installed.

Therefore, an operator's customized mobile phone usually requires the priority of the route to be modified so that the priority of the SE (SWP-SIM) route is better. That is, if the same AID application exists, the route will be preferentially routed to the SWP-SIM. Handle to ensure compatibility with old-release SE-enabled devices after system upgrade to 4.4.

The doubts about mobile payment will be even more amplified on Android Pay. Because Android is friendly to developers all over the world, it adopts an open system and whether such an open environment may lead to malicious intrusion opportunities. Just like Samsung Pay, Android Pay cannot be used for devices that have already been rooted, unless the user bypasses the Root's checking mechanism through tools. In addition, Android Pay also improves the security through HCE and Token services. HCE refers to host card emulation, which replaces the hardware security components with software emulation and puts user data in the cloud. Simplify the payment process,

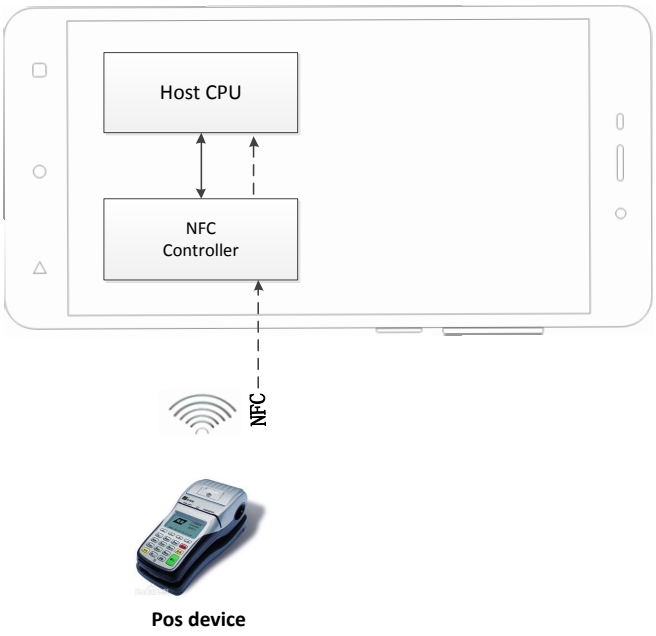

Fig. 30. NFC card emulation without a secure element.

D. Apple pay

Apple Pay only supports NFC payments, and its technology is very similar to Samsung's NFC technology. Since it does not support the magnetic stripe payment, many older devices that only support magnetic stripe payments cannot use Apple pay. Therefore, Apple's payment is more limited than Samsung's payment.

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, but are limited to only supporting their own models, and their audiences are relatively Narrower.

Apple's core technology is still Tokenization. Not only that, Apple is also one of the promoters of the Payment Token specification.Although almost all foreign or domestic analysis articles have intentionally or unintentionally mentioned that Apple Pay has implemented the EMVCo specification, so far no official information from Apple or EMVCo has mentioned that Apple Pay has implemented the Tokenisation specification of EMVCo, but The process of adding a card to Apple Pay is very similar to that of EMVCo's request token. At this time, Apple plays the role of a token requester (the specification of EMVCo explicitly mentions that the device manufacturer that makes mobile payment can be One of the main categories of token requestors), the bank or payment network plays the role of a token service provider. In addition, the dynamic security code that provides basic security for Apple Pay transactions is very similar to the method of generating and using the Token Cryptogram of the EMVCo specification. Rethinking that Visa and MasterCard have disclosed their tokenization services after the launch of Apple Pay, we have reason to believe that Apple Pay actually implements the Tokenisation specification of EMVCo.

Like the Samsung, the ios system has an application called wallet. When you bind a card, you need to connect to an Apple Pay server. Similarly, the Apple Pay server will also request the virtual bank card from the bank or card organization server with the bank card information submitted by the user.

The mobile phone and Apple Pay server do not save the full bank card number, and only store the unique Device Account Number in the SE. (The payment credentials generated by DAN's iPhone device information and Token encryption can effectively prevent the leakage of credit card information.

Apple Pay is a product that integrates various technologies and resources. Its composition is more complex. The core components include:

Embedded Secure Element: As described in section 3.

NFC controller: NFC controller. In the context of Apple Pay, the NFC controller acts as a router. It is connected to three different external entities: external near-field devices (eg, point-of-sale (POS), point-of-sale), and applications. The processor (AP, Application Processor) and Secure Element, in turn, form two communication channels: the application processor's communication channel to the Secure Element, and the communication channel between the POS and the Secure Element.

Wallet: The Wallet was originally called the passbook and was renamed wallet after IOS 9. It was a service that existed before the Apple Pay product was released. After Apple Pay was released, Apple expanded its functionality to allow it to add and manage credit cards and debit cards for Apple Pay.Of course, It can also check the added card information, the bank's privacy policy, and recent transaction details. For Apple Pay, Wallet is equivalent to the management client of Secure Element. Adding or deleting card or debit card information in Secure Element can be performed via the Wallet service.

Touch ID: This is the iPhone's fingerprint recognition service. Its purpose is to use fingerprint recognition to make access to the device more secure, faster, and easier. Touch ID is not a replacement of the device security password, but allows users to use complex device passwords without sacrificing convenience. In other words, users can use complex passwords to protect the device while also using the Touch ID to easily access the device.

Secure Enclave: Secure Enclave is an internal secure execution environment for iOS devices. It can be used to process sensitive information. For example, the data acquired by Touch ID's fingerprint imaging sensor needs to be passed to Secure Enclave for the actual fingerprinting process. For Apple Pay, Secure Element manages the certification process and makes payment transactions possible. Secure Enclave is a coprocessor packaged together by the Apple A7 and subsequent series of application processors. It has its own secure boot process and personalized software update process, and it is separate from the application processor where the iOS system is located. Secure Enclave uses encryption (using a temporary generated key encryption) physical memory (a portion of the physical memory shared by the application processor) for business processing and has its own hardware random number generator. Secure Enclave communicates with the application processor through the interrupt-driven mailbox and shared memory, and provides all cryptographic services related to data protection key management.

Apple has never mentioned that Secure Enclave is an implementation of the ARM TrustZone security extension technology (although according to the description of several secure communication channels in the official Apple documentation, Secure Enclave is probably an implementation of the ARM TrustZone technology), we are still It is impossible to determine whether the Secure Enclave is an independent coprocessor or an application processor running state (both architectures can provide the required security features of Secure Enclave), this needs to be announced by Apple for more details of the implementation of Secure Enclave, At present, it can be concluded that the security features provided by Secure Enclave can also be implemented

*1) Communication security between Secure Enclave and Touch ID:*We know that the fingerprint data acquired by the Touch ID imaging array needs to be actually matched by the Secure Enclave. In the implementation of Apple Pay, the Touch ID sensor is connected to the application processor through the serial peripheral interface bus (Serial Peripheral Interface Bus). Connect and then connect to the Secure Enclave. In other words, the fingerprint imaging data acquired by

the fingerprint sensor needs to be relayed via the application processor. This poses a security risk: malicious programs can intercept the data generated by the Touch ID sensor. Apple Pay realizes the secure transmission of fingerprint data in a simple way. First, the Touch ID sensor and Secure Enclave will preset a shared key, then use the shared key to negotiate a session key, and then use the negotiated session key to use. The AES-CCM algorithm encrypts the transmitted data. This ensures that the application processor cannot read fingerprint data and ensures the security of the entire fingerprinting process.

2) Communication security between Secure Enclave and Secure Element: As mentioned earlier when the NFC controller was introduced, the physical communication channel between the Secure Enclave and the Secure Element needs to be relayed through the NFC controller. There is no direct physical connection between the two, which is specifically the Secure Element and NFC controller. Connected, and then the NFC controller is connected to the application processor without mentioning how the NFC controller is connected to the Secure Enclave (as stated by Apple's official documentation, it can be seen here that the Secure Enclave is probably not a separate coprocessor), Then, since Secure Element and Secure Enclave need to transit through the application processor, it is necessary to consider the communication security.

The implementation is similar to the process of communicating with Touch ID and Secure Enclave. It also encrypts the communication content by sharing the pairing key. However, because the Secure Element is involved, the preset of the shared pairing key is more complicated, specifically: The pairing key is preset at the production stage, and the key is generated by the Secure Enclave using its own UID key and the unique identifier of the Secure Element as input, and then securely transmitted to the external hardware security module (HSM, Hardware) in the factory. Security Module) and then injected into Secure Element. In actual use, the communication between Secure Element and Secure Enclave is encrypted using an AES-based cryptographic algorithm, and a cryptographic mechanism is used to prevent replay attacks.

Apple Pay Servers: Apple Pay Server, which manages the status of credit and debit cards in Passbooks as well as device-specific account information stored in Secure Element. The Apple Pay server communicates with both the device and the server in the Payment Network. For in-app payments, the Apple Pay server is also responsible for using merchant-specific keys and Payment Credentials for Apple Pay. Encrypt it and send it to the actual merchant server for payment processing.

using ARM TrustZone technology.

IX. 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.

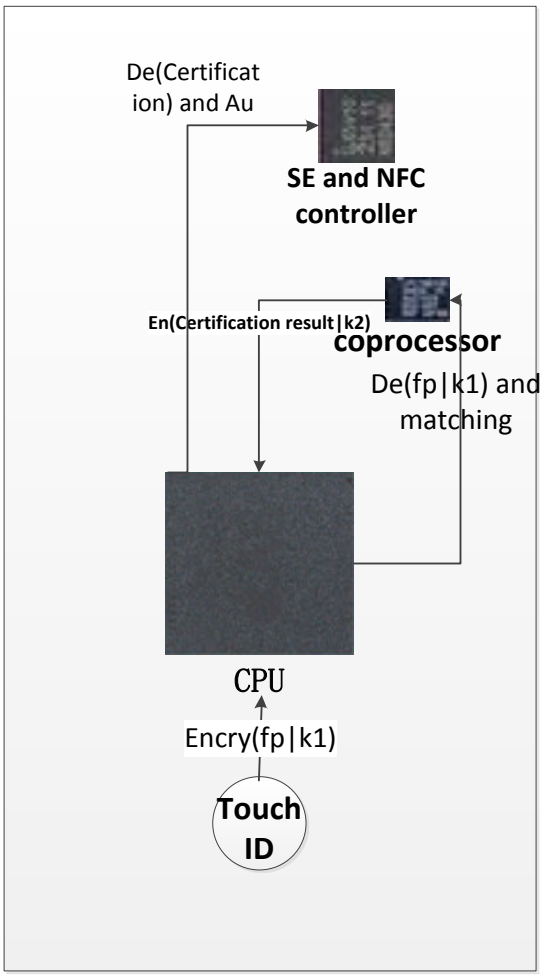

Fig. 31. Apple pay for payment.

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.

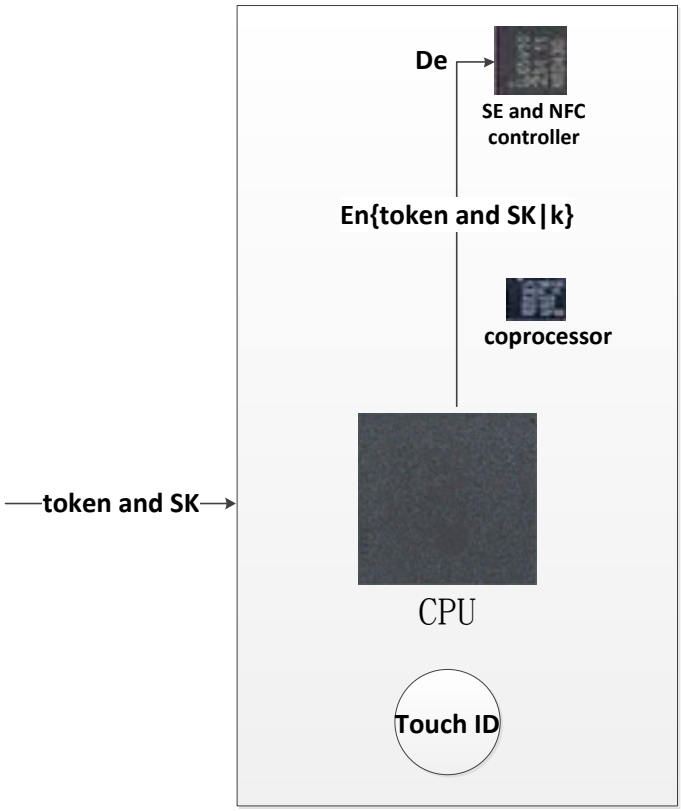

Fig. 32. Apple pay for token application.

[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.

[15] Alves T. *TrustZone : Integrated Hardware and Software Security[J]. White Paper*, 2004.

[16] Kanniainen L. *Alternatives for banks to offer secure mobile payments[J].* International Journal of Bank Marketing, 2010, 28(5):433-444.

[17] Coskun V, Ozdenizci B, Ok K. *A Survey on Near Field Communication (NFC) Technology[J].* Wireless Personal Communications, 2013, 71(3):2259-2294.

[18] Reveilhac M, Pasquet M. *Promising Secure Element Alternatives for NFC Technology[C].*International Workshop on Near Field Communication. IEEE, 2009:75-80.

[19] Micro Focus, *Secure Stateless Tokenization (SST)*, Available at "http://files.asset.microfocus.com/4aa6-5576/en/4aa6-5576.pdf".

[20] Terence Spies, Mountain View, CA(US),Richard T.Minner, Carmichael, CA(US), *system for protecting sensitive data with distributed tokenization*, US 8595850 B2, 2013-11-26.

[21] Ulf Mattsson, Stamford, CT(US), *distributed tokenization using several substitution steps*, US 8745094 B2, 2014-6-3.

[22] Ulf Mattsson, Cos Cob,CT(US), Yigal Rozenberg, Wilton, CT(US),Vichai Levy, Norwalk, CT(US), *table-connected tokenization*, US 9237006 B2, 2016-1-12.

[23] Nojiri T. *Two-dimensional code, methods and apparatuses for generating, displaying and reading the same*: US, US 7032823 B2[P]. 2006.

[24] Hara M, Watabe M. *Two dimensional code reading apparatus*: EP, US 5691527 A[P]. 1997.

[25] Hara, Masahiro, Watabe, Motoaki, Nojiri, Tadao , Nagaya, Takayuki, Uchiyama, Yuji.*Optically readable two-dimensional code and method and apparatus using the same*:US 5726435. 1995.

[26] Coskun V, Ozdenizci B, Ok K. *A Survey on Near Field Communication (NFC) Technology[M].* Kluwer Academic Publishers, 2013.

[27] Vedat Coskun, Busra Ozdenizci, Kerem Ok. *The Survey on Near Field Communication[J].* 2015, 15(6):13348-13405.

[28] Brown, T.W.C.; Diakos, T. *On the Design of NFC Antennas for Contactless Payment Applications*. In Proceedings of the 5th European Conference on Antennas and Propagation (EUCAP), Rome, Italy, 1115 April 2011; pp. 4447.

[29] Gebhart, M.; Szoncso, R. O*ptimizing Design of Smaller Antennas for Proximity Transponders*. In Proceedings of the IEEE Second International Workshop on Near Field Communication, Monaco, 20 April 2010; pp. 7782.

[30] Coskun V, Ozdenizci B, Ok K. *A Survey on Near Field Communication (NFC) Technology[J].* Wireless Personal Communications, 2013, 71(3):2259-2294.

[31] Coskun V, Ok K, Ozdenizci B. *Near Field Communication (NFC): From Theory to Practice[J].* 2012, 13(March 10):816-825.

[32] Roland M, Langer J. D, *igital Signature Records for the NFC Data Exchange Format[C]// Second International Workshop on Near Field Communication*. IEEE, 2010:71-76.

[33] Aziza H. *NFC Technology in Mobile Phone Next-Generation Services[C]*, Second International Workshop on Near Field Communication. IEEE Computer Society, 2010:21-26.

[34] Luca G D, Lillo P, Mainetti L, et al. *The use of NFC and Android technologies to enable a KNX-based smart home[C]*, International Conference on Software, Telecommunications and Computer Networks. IEEE, 2013:1-7.

[35] Coskun V, Ok K, Ozdenizci B. *Professional NFC Application Development for Android[M].* Wiley, 2013.

[36] Plos T, Hutter M, Cavaliere F, et al. *Security-Enabled Near-Field Communication Tag With Flexible Architecture Supporting Asymmetric Cryptography[J].* IEEE Transactions on Very Large Scale Integration Systems, 2013, 21(11):1965-1974.

[37] Agbinya J I, Selvaraj N, Ollett A, et al. *SIZE AND CHARACTERISTICS OF THE 'CONE OF SILENCE' IN NEAR-FIELD MAGNETIC INDUCTION COMMUNICATIONS[J].* Annual report of Institute of Disaster Prevention, Kyoto University, 2009, 2:p621-640.

[38] Agbinya J I. *Power Equations and Capacity Performance of Magnetic Induction Communication Systems[J].* Wireless Personal Communications, 2012, 64(4):831-845.

[39] Coskun V, Ok K, Ozdenizci B. *Near Field Communication (NFC): From Theory to Practice[J].* 2012, 13(March 10):816-825.

[40] Coskun V, Ok K, Ozdenizci B. *Professional NFC Application Development for Android[J].* Wiley John + Sons, 2013.

[41] ETSI TS 102 613, Smart Cards; UICC - Contactless Front-end (CLF) Interface; Part 1: Physical and data link layer characteristics, Technical Specification, ETSI TS. Available online:http://www.etsi.org/deliver/etsi_ts/102600_102699/102613/07.03.00_60/ts_102613v070300p.pdf(accessed on 13 April 2015).

[42] ECMA 373: Near Field Communication Wired Interface (NFC-WI), ECMA International.Available online:http://www.ecma-international.org/publications/standards/Ecma-373.htm (accessed on 13 April 2015).

[43] NFC Stepping Stones 2011, SIM Alliance, White Paper. Available online: http://simalliance.org/nfc/nfc-technical-releases/ (accessed on 13 April 2015).

[44] NFC Analog, NFC Forum, Technical Specification. Available online: http://nfc-forum.org/our-work/specifications-and-application-documents/ (accessed on 13 April 2015).

[45] NFC Digital Protocol, NFC Forum, Technical Specification. Available online: http://nfc-forum.org/our-work/specifications-and-application-documents/ (accessed on 13 April 2015).

[46] NFC Activity, NFC Forum, Technical Specification. Available online: http://nfc-forum.org/our-work/specifications-and-application-documents/ (accessed on 13 April 2015).

[47] Xiaolong Bai and Zhe Zhou and XiaoFeng Wang and Zhou Li and Xianghang Mi and Nan Zhang and Tongxin Li and Shi-Min Hu and Kehuan Zhang, *Picking Up My Tab: Understanding and Mitigating Synchronized Token Lifting and Spending in Mobile Payment*, 26th USENIX Security Symposium (USENIX Security 17), 2017, 978-1-931971-40-9, Vancouver, BC, 593–608, https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/bai,USENIX Association.

PLACE PHOTO HERE

Michael Shell Biography text here.

John Doe Biography text here.

Jane Doe Biography text here.