Thi My Anh Tran

MOBILE PAYMENT SECURITY
A case study of Digital Wallet MOMO

Bachelor's thesis

Information Technology

Bachelor of Engineering

2020

XAMK
South-Eastern Finland
University of Applied Sciences

XAMK
South-Eastern Finland
University of Applied Sciences

Author (authors)	**Degree title**	**Time**
Thi My Anh Tran	Bachelor of Engineering	May 2020

Thesis title

Mobile Payment Security
A case study of Digital Wallet MOMO

78 pages
1 page of appendices

Commissioned by

Supervisor

Matti Juutilainen

Abstract

The objective of the thesis was to conduct a security testing on MOMO, the most popular digital wallet in Vietnam. The goal was to determine the efficiency of security technologies that are applied by MOMO.

In order to investigate the problem, theoretical research and studies were made based on the working and security principles of mobile payment and e-wallet. The thesis also aimed to broaden knowledge and provide deep understanding of mobile payment. This study explored (i) different types of mobile payment in terms of technology, advantages and disadvantages, (ii) the benefits and drawbacks of mobile payment in comparison to traditional payment, (iii) the threat model associated with all stakeholders involved in the mobile payment, (iv) security measures towards each stakeholder, and (v) security testing in MOMO e-wallet with OWASP Top 10 as the primary guideline.

Quantitative research methods alongside the experiments were used to identify the security threats that are considered as vulnerabilities in mobile payment. The primary data were collected to get familiar with the target (MOMO) and perform the security evaluation in practice. The analysis was done for each security risk with a separate framework to be used. Based upon the summary of the security test result, the identified factors were considered as certain suitable lessons learned to improve m-commerce in the future.

Research findings highlighted the diverse and constant development of mobile payment. The study examined the security mechanism of MOMO and verified the security system. The thesis contributes to a better understanding of mobile payment and digital wallet security. The study can be a reference for further mobile payment Security study and MOMO security enhancement.

Keywords

Mobile payment, digital wallet, security, m-commerce

CONTENTS

TERMINOLOGY

RFID	Radio Frequency Identification
NFC	Near Field Communication
SMS	Short Message Service
P2P	Peer-to-peer
B2C	Business to Consumer
C2B	Consumer to Business
QR code	Quick Response code
WAP	Wireless Application Protocol
POS	Point Of Sale
PIN	Personal Identification Number
ECMA	European Computer Manufacturers Association
MST	Magnetic Secure Transmission
NSDT	Near Sound Data Transfer
MMS	Multi Messaging Service
USSD	Unstructured Supplementary Service Data
UX	User Experience Design
UI	User Interface Design
SFA	Single Factor Authentication
MFA	Multi-Factor Authentication
ID	Identity Document
ATM	Automated Teller Machine
PKI	Public-key Infrastructure
OTP	One-time Password
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
PCI DSS	Payment Card Industry Data Security Standard
EMV	Europay, Mastercard, and Visa
PAN	Primary Account Number
HVT	High Value Tokens
LVT	Low Value Tokens
DNA	Deoxyribonucleic Acid
DES	Data Encryption Standard

NIST	National Institute of Standards and Technology
AES	Advanced Encryption Standard
RSA	Rivest–Shamir–Adleman
GCHQ	Government Communications Headquarters
CA	Certificate Authority
RA	Registration Authority
VA	Validity Authority
SSL	Secure Socket Layer
TLS	Transport Layer Security
MD5	Message Digest 5
SHA	Secure Hash Algorithm
SET	Secure Electronic Transaction
API	Application Programming Interface
LAN	Local Area Network
POI	Point of interaction
MiTM	Man-in-the-middle
PTP	Point-to-point
PSP	Payment Service Provider
DoS	Denial of Service
GSMA	Global System for Mobile Communications
R&D	Research & Development
2FA	Two-factor Authentication
TCP	Transmission Control Protocol
OSI	Open Systems Interconnection
OWASP	Open Web Application Security Project
VCT	Virtual Card Technology
AI	Artificial Intelligence
VR	Virtual Reality

1 INTRODUCTION

Together with the significant increase in the number of smartphone users, more and more people these days are choosing mobile payment as their primary payment method. Mobile payment, or in short, e-wallet, has become popular during the 2010s, and will definitely continue to be even more popular in the near future. The rise of mobile payment can be seen easily everywhere all over the world.

It is extremely convenient to have your card integrated to your phone, and digitally view your transaction anywhere. No more taking time counting each penny, waiting for the change, or bringing a thick wallet with you. The use of mobile payment has also been proven to contribute to lowering the rate of pickpocketing, or counterfeit money handling (Ryan 2014). Some high-developed countries, such as Sweden, Norway and Iceland, have reached a level as a cashless environment (David 2019; Deloitte 2019). As we are stepping into the digital world, the development of mobile payment is unavoidable and will bring many noticeable benefits to our world. Moreover, it is predicted that mobile payment will gradually change the whole world’s cashflow. Despite many existing concerns about its technology and security, e-wallet indeed will have a big impact in our life.

The biggest concern of customers when it comes to mobile payment is its convenience and security. While mobile payment is offering outstanding convenience for purchasing goods and services, the security of the system is still in doubt. Data privacy and fraud risks put people off adopting mobile payment. Many researches and studies were carried out to improve the security of mobile payment generally and digital wallet specifically. Every new feature and function that are added to this application should be tested to ensure proper work in any customer’s use cases and maintain the best quality of customer experience. Therefore, security tests are crucial to enhance the security system, identify vulnerabilities and develop new security technologies in the long term.

The practical aim of the thesis is to investigate the security measures of MOMO, one of the most popular mobile wallets in Vietnam. It is favoured because of high security standard and excellent customer service response. Theoretical study on mobile payment and digital wallet provides thorough insights over the security mechanism and understanding to prepare for the security testing.

In order to accomplish the set goals, quantitative methods are used throughout the study. The structure of the thesis is as follows:

- **Chapter 1** (*Introduction*) is the introduction about the objective and goal of this thesis.
- **Chapter 2** (*About Mobile Payment*) includes theory gathering and research on the documentation about mobile payment, different types in terms of technology, the advantages and disadvantages of mobile payment.
- **Chapter 3** (*Mobile Wallet Security*) introduces the common technologies to be used in digital wallet security and their working principles. Moreover, the threat model is explained and security measures are recommended for each stakeholder.
- **Chapter 4** (*Case Study of MOMO*) is a brief introduction about MOMO e-wallet and its achievements. MOMO's security features are explained as well. The testing guidelines from Open Web Application Security Project (OWASP) are referenced in the end of this chapter.
- **Chapter 5** (*Security Testing in MOMO*) consists of a separate analysis and experiment to verify different security risks using many frameworks. The result of the experiment is considered as proof of high security standard and contributes to further security improvement.
- **Chapter 6** (*Future Technology*) shows predictions about new security technology. This chapter includes both the opportunities and challenges of mobile payment in the future.
- **Chapter 7** (*Conclusion*) presents the summary of the analysis and experiment that are conducted with MOMO to provide further

understanding of mobile payment & digital wallet security and hand on practice.

At the end of the thesis, the efficiency of security technologies applied by MOMO is verified from the theoretical research and the result of the security testing. The study will contribute to improve mobile payment security in the future.

The primary knowledge about mobile payment will be introduced in the next chapter.

2 MOBILE PAYMENT OVERVIEW

This chapter covers basic knowledge and understanding of: mobile payment's definition and history overview, different types of mobile payment regarding the technology implemented, and the comparison between the traditional payment and mobile payment. The study on this chapter will provide sufficient knowledge in the theoretical part and better guiding for the practical part in the 5th chapter.

2.1 Definition

According to Thomas (2013), mobile payment (also known as mobile money, mobile wallet, e-wallet, digital wallet) is the payment service that is performed via a mobile device under all financial regulations. It is different from the traditional payment where consumers use their cash, credit card or cheque to checkout for goods, service or online payment. By this way, consumers do not need to bring along a separate payment element, but only their smartphone which includes digital payment software. Although the concept of maintaining a non-note-based (cashless) payment system has emerged long ago, it was only in the 2010s that we could witness the rapid adoption of mobile payment for daily purchasing (Matthew 2012).

Mobile payment has a big influence on the economy. It eases the complexity of micropayments. It extends the use of financial payment within the community. It pushes the number of transactions made per day by introducing new secure and convenient features. It approaches more targeted financial customers and improves the business volume. Mobile payment also allows more purchasing options regarding consumer’s payment choices. Mobile payment has changed the interface of payment system, initiating immediate authorized and secure, encrypted transactions. There is no doubt that m-payment will moderately replace the manual, errable payment model. (Thomas 2013.)

2.2 History of Mobile Payment

The description of this section about the history of mobile payment bases on the discussion of Flavio (2015) and John (2016).

Throughout history, human beings have constantly created different sorts of payment system. They have evolved from exchanging goods and livestock such as grains, shells, meat, cattle, silk, etc. in the Stone Age (around 9000-12000 B.C.) to the appearance of simple metal coins in Asia around 2000 B.C. In 960, China was the first to introduce money in the form of paper under the Song dynasty. This started a new phase in the development of payment process and banknote is still the most common type of money nowadays. Despite being first mentioned by Edward Bellamy’s “Looking Backward” of 1887, it was not until 1921 that a charge card was issued to customers of Western Union. The credit card, which we are all familiar with in daily life, has rooted from a modern credit card by a third-party bank called Bank Americard in 1958. It was renamed Visa in 1977, and resembled the Visa Card that we mostly see in the 21st century. Today, the concept of money varies with all forms, cash, card, cheque, and most recently, electronic wallet.

The history of mobile payment has been dated back in 1997, when Coca Cola allowed their customers to purchase drink via mobile in Helsinki. Coca Cola set up a vending machine so that people could send a text message to select and purchase their drink. In the meantime, RFID (Radio Frequency Identification) was introduced by ExxonMobile as a keyring and swiped to pay instantly at the pump. This Speedpass is the first contactless payment to be made at that time. Beginning with the rapid growth of mobile users and high technology, the development of Web payment evolves into the current wave mobile payment, or digital wallet. Online banking was believed to be first in use by Pizza Hut in 1994. In 1999, Ericsson made it possible to purchase movie tickets via mobile phones. The number of cell phone users who made online payment rose to 95 million in 2003. In 2008, Apple and Android started opening their Appstore to third-party developers, offering an opportunity for building marvelous amounts of applications. To people's surprise, the first digital wallet comes from Google. Google Wallet set the very first step to the market. Nevertheless, it has some limitations due to the fact that it is only used on one particular model and accepted by few merchants. But thanks to the awaiting release of Apple Pay in 2014, followed by Samsung Pay a year later, digital wallet set its step to the market and played a significant role in the revolution of mobile payment. It involved the majority of mobile users to start using those Pays application for the purchase. The first and favorite merchants were Starbucks, Walmart, and Dunkin Donuts.

Just as essential as the other benefits that a smartphone introduced, mobile payment has nearly become a must-have app, especially among young people. Some processing models applied can be named such as Near-Field Communication NFC (widely known as contactless payment), Carrier billing (SMS and direct billing), Mobile Wallet, Card based payment and Direct transfer between payer and payee in near real time. Among the above models, mobile wallet is the outstanding signature of the digital world. It is an application that allows users to purchase their goods and service directly via mobile phones. There is a variety of functional application for mobile payment. We are mainly familiar with big player such as Apple Pay (from iOS devices), Alipay (generated by Alibaba and widely used in China), Google Pay, Samsung Pay and WeChat Pay. In Vietnam, the biggest e-wallet provider is MOMO, a product of the Fintech company M_Service. This study will later introduce security features that contribute to the success of this startup.

According to Venkatesen (2013) and Instituto Economía Digital ESIC (2016), there are two primary types of mobile payment in terms of technology to be used:

proximally and remotely. Each consists of many different technologies to perform successful P2P, B2C (Business to Consumer) or C2B (Consumer to Business) transactions via mobile activity. The variety of mobile payment type provides users with most convenience while purchasing their goods and services. Proximity and remote payment differ by distance between user's devices and merchant's terminal. Proximity payment's principle bases on technologies such as NFC, QR code and chip-based devices. On the other hand, remote payment refers to Short Message SMS, Wireless Application Protocol (WAP), web browsers and mobile applications. No matter what technology is used, where it is performed or how much the transaction costs, the mobile operator and the bank must ensure that the mobile application makes correct decisions regarding the customer's financial account and the payment is verified.

2.3 Proximity Payment

Proximity payment refers to the most common payment method we often see with mobile devices from a close distance. One can purchase at available POS (Point of Sale) in stores or at vending machines by an NFC-enabled mobile phone. It will carry and load encrypted data in a secure way, the same as contactless payment cards.

2.3.1 Digital Wallet

The concept of e-wallet has emerged long ago in the online commerce. Pay Pal was the first to support digital wallet for the major online commerce, eBay, at the time. The launch of Apple Pay in 2014 broadened digital wallet's place in the financial market.

Over 50% of the young generation uses mobile wallet as their primary payment method (Jaime 2019). Figure 1 shows that in 2019, there are many digital wallet choices coming from large corporations such as Apple Pay, Google Wallet, Alipay, Samsung Pay, Wechat Pay, etc.

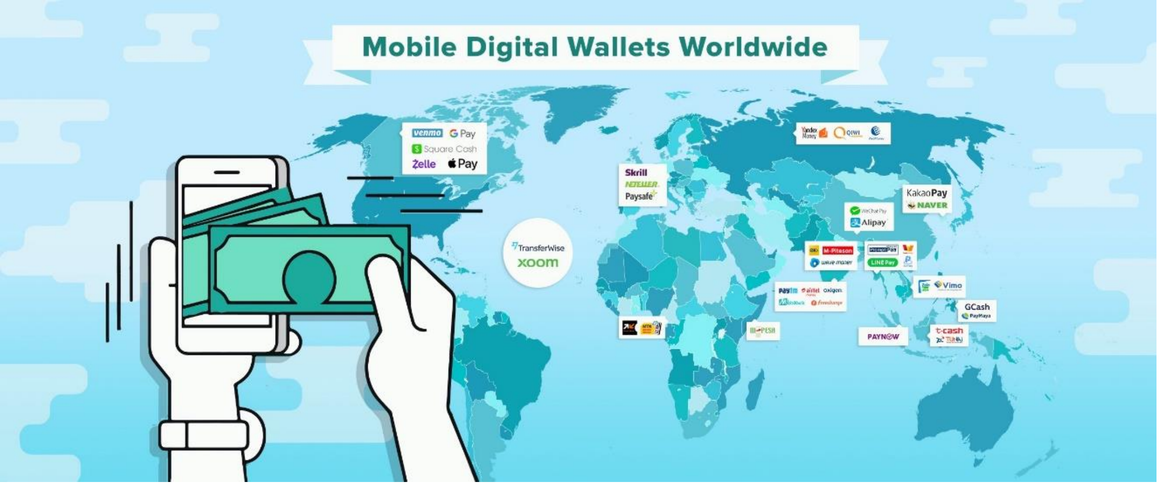


Figure 1. Mobile Digital Wallet Worldwide 2019 (medium.com)

A mobile wallet is a mobile application that contains information on user's credit and debit card so that it can act likewise and let users make payment by "tap-and-go". The process includes the following steps:

- User installs the app and authenticates identity by PIN number which is sent through.
- User inputs their credit card details and generates an account on the mobile wallet that is linked to its financial bank account or credit card.
- User can validate the payment securely every time they purchase (requires PIN input).

Figure 2 also indicates countries with highest adoption rate of mobile payment:

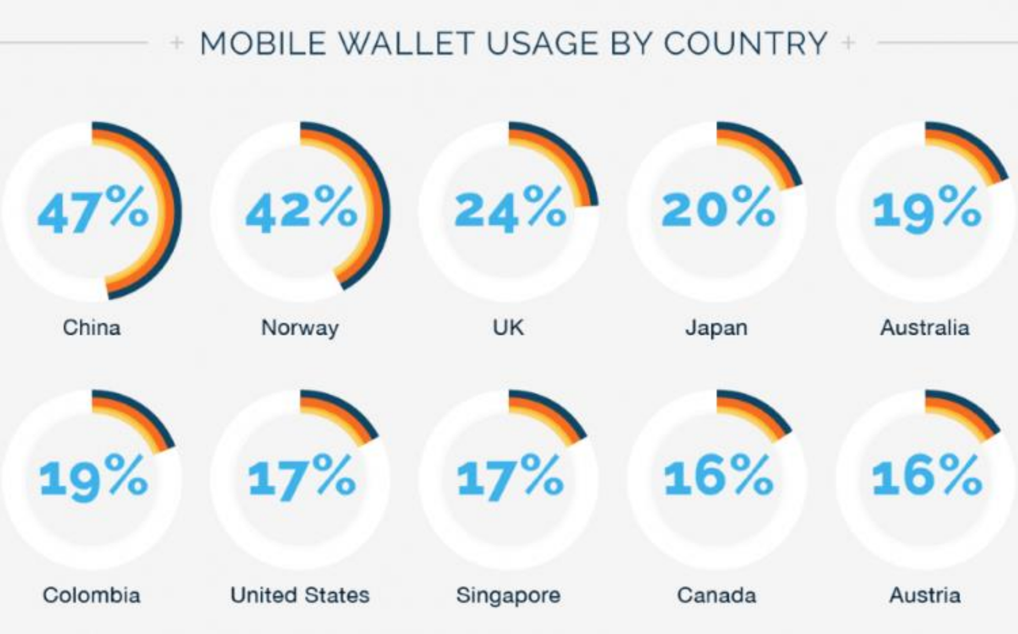


Figure 2. Mobile Wallet Usage by Country (scandasia.com)

According to Guo (2016), digital wallets are categorized into four types as folows:

- **Open wallet** can be used freely to purchase goods, services and other financial transactions such as funds transfer, cash withdrawal.
- **Semi-open wallet** can be used to buy items and services at merchants' POS, but unable to allow consumers to withdraw cash.
- **Closed wallet** is a specific software application that is built only for the use of a particular brand or store. For example, Walmart Pay and Amazon Pay are designed exclusively for facilitating the purchase for a single vendor. Closed wallet does not permit cash withdrawal or redemption.
- **Semi-closed wallet** can be used for buying goods and services, performing financial activities at a selected number of merchants or outlets. Semi-closed wallet covers certain locations that have contracts with an issuer to accept this payment instruments. This kind of wallet cannot be used to withdraw money either.

Digital payment eliminates the complex, time-consuming traditional and other m-payment, allows individuals to purchase items quickly or fund-transfer to friends and family.

The benefits and drawbacks of digital wallet are explained by MyAccountGo (2019) as follows.

Benefits:

- **Low cost:** Digital wallet eliminates intermediates, therefore reducing the cost adoption and implementation.
- **Convenience**: With user's card integrated to the mobile phone, they can make purchases easily and hassle-free.
- **Increase revenue:** Since it is very convenient to use, digital wallet promotes the growth of business markets, introduces mobile payment to places where only traditional cash was accepted before, for example at flea markets, craft fairs, etc.

Drawbacks:

- **Security**: Inputting the cardholder’s information to a device can expose potential security hole to user’s personal data.
- **Mobile phone dependency:** Consumers are reliant on their phone to function normally. In case the phone runs out of battery or goes missing, users will be left with no digital wallet.
- **Limited options**: Users may be tied to a number of digital wallet providers depending on the partnership the wallet has with other merchants.

In the digitalized world, it is forecasted that the payment value that is stored in digital form causes a wind of change.

2.3.2 QR Code Payment

Together with the increasing number of smartphone users, there are more and more QR code payments to be made. QR, or Quick Response, is a square bar code that is digitally created and valid to pay after scanning. There are two ways to perform scanning with QR code:

- It can be displayed on the mobile device of the payer and scanned by Point of sale (POS) from the payee side.
- It can be displayed by the payee and the payer scans the code with their mobile phone to execute the payment.

QR code payment is contactless payment. It abandons many elements in bulky infrastructure associated with electronic payment, for example payment cards, terminals and merchant registration. The first mobile wallet app allowing payment with QR code was launched in 2012. Tencent, an enormous Chinese Fintech company, put QR code into common use through an application called WeChat. Since then, QR code Payment has brought out a lot of benefits to the m-commerce market (Derrick 2017):

- **Easy implementation:** QR Code does not require complicated process to launch the application.

- **Simplicity:** QR code is generated in less than a second and easy to use. The customer just needs to have it scanned and make the purchase within a minute.
- **Fast**: It has quick response so that consumers can view and make payment simultaneously without any delay.
- **Convenience:** All transaction information including the bank account number, value and title are automatically filled in. This reduces manual steps, increases accurateness, and saves precious time for the user.
- **Security:** The security implemented in QR Code Payment follows high standards and safety regulations.

Despite its simplicity, this payment method can expose some security holes, mostly related to malware QR code that can contain malware or Trojans.

2.3.3 NFC Contactless Payment

NFC is the most well-known technology in contactless payment. It is a protocol that enables two electronic devices to store, exchange and transmit data between each other. The devices must be kept at a close range to get NFC effective. User can make payment easily as long as they keep their NFC-enabled devices near a reader module or POS. NFC portable devices can also read, store, and write data inductively thanks to NFC tags. Identity authentication might be required using PIN to ensure secure payment information. Users tend to prefer NFC over other payment systems due to its highly encrypted data and ease of use.

The emergence of NFC rooted from Radio Frequency Identification technology (RFID) in which compatible devices can communicate via electronic tags using radio waves. In 2003, NFC was officially approved as ISO/EIC standard, and nowadays, ECMA standard. NFC was first in use on a Nokia model 5140 device. In 2009, P2P communication was leveled up thanks to Bluetooth initiation. NFC smart tags were introduced by Sony in 2012, which made way for the first NFC-based financial transaction in November 2015. Today, almost all mobile payment is made based on NFC technology. (ECMA 2013.)

NFC technology offers some benefits along some drawbacks as follows:

Benefits:

- **Versatility**: NFC can serve any kind of services, for instance, bank cards, travel cards, movie tickets, keycards, etc.
- **Security:** NFC is much more secure than a traditional magnetic strip card. NFC abandons the physical access from merchant to the credit card. Moreover, the transaction is a well-secured and established encrypted data channel.
- **Convenience:** NFC is a time-saving technology that is critical in our modern world. No one would have to endure a big queue of lines waiting to checkout while going shopping.
- **Low cost:** NFC connection requires simple set up to capture wireless signal. Therefore, it is a wise investment for both users and merchants.

Drawbacks:

- **Security issues**: NFC is prone to man-in-the-middle attacks. Hackers can establish a specific key to perform eavesdropping or data modification. RF signal can be picked up with an antenna and exposed to possible relay attack.
- **Incompatible hardware**: If vendors do not integrate NFC into their devices, consumers are not able to pay with this technology.
- **Data privacy:** Because credit card information is stored on the phone, phone hacking could expose this sensitive payment data.

Scientists are working hard to improve the disadvantages of NFC technology in order to make more use of it in other applications.

2.3.4 Sound Wave Payment

Sound wave, or signal wave is a new technology that works on various devices such as smartphones, swipe cards and POS terminals. Sound wave payment enables contactless payment by transmitting data through soundwaves.

Soundwaves will be sent from the POS terminal to mobile phones and these signals will be later converted into analog. (Comviva 2016.)

Transactions are processed without the need of the Internet. Therefore, it is an affordable solution for remote areas and countries that still rely on basic technology.

The benefits and drawbacks that Sound wave payment introduces are as below:
Benefits:

- **Compatibility:** Sound wave payment is compatible with all hardware devices.
- **Support for a wide range of customers**: Sound wave payment does not require Internet access and any specific platform, therefore it can approach more targeted customers.
- **Low cost:** Little or no extra cost for merchants will increase the adoption rate
- **Convenience:** Easy to use, no complex interaction.
- **Better customer experience:** Better experience with real time updates.
- **Effortless transactions**: Quick, relevant and reliable payment data to be processed.
- **Security:** Data is encrypted and and a secure channel is established to transmit information.

Its platform-independence makes it increasingly popular in mobile payment market. Sound wave payment can support wider ecosystem. In addition to payment at the merchant’s POS, sound wave payment can also be used as P2P mobile money transfer. Recently, Alipay, the largest mobile payment company in China, released a new sound wave payment mobile product. This will be the sign for the potential growth of this technology in the future.

2.3.5 Magnetic Secure Transmission (MST)

Another technology that is applied in mobile payment systems is Magnetic Secure Transmission. MST has been powered by Samsung Pay service since 2015. Though not as common as NFC, both of these two technologies are quite similar. NFC and MST are classified as contactless payment which does not require physical interaction with the merchant's terminal. The unique difference is in MST Technology, magnetic signals are emitted to generate the connection between the user's mobile devices and the merchant's terminal. The magnetic signal is later transmitted (as if a physical card is swiped) from your device to the card reader for further processing. (Emily 2018.)

MST picks out the best features of NFC and traditional card payment. People can make use of the existing card reader without any software or hardware upgrade. MST is demonstrated as secure as NFC, and safer than the traditional physical card. This is considered a thorough alternative solution for mobile payment.

2.3.6 Cloud-based Mobile Payment

The ever-increasing number of cloud services during the last few years has led to a new level of mobile payment. To make use of the convenience and simplicity of cloud computing in payment systems, Google Wallet, Paypal, GlobalPay, GoPago etc. developed the cloud-based approach for in-store payment.

This technology initiates two separate transactions, placing the mobile payment provider in the middle of the transaction. Firstly, users are free to select a cloud-linked method and authorize the payment, usually via NFC. The charge will be automatically covered by the payment provider. In the second transaction, the payment provider gets the fee back from the purchaser's cloud-linked account. (ACCEO Tender Retail Team 2017.)

Cloud-based mobile payment introduces some benefits and drawbacks as below:
Benefits:

- **No Single Point of Failure** in cloud environment

- **Convenience:** Easy to use from the user’s perspective
- **Flexible business model**: Open opportunities to deploy service for providers
- **Issuer Brand value**: Direct control over branding and user experience
- **No ecosystem dependency**: Less intermediates, less security breaches
- **Speed**: Fast time-to-serve product and service
- **Security**: Secure channel authorized by approved vendors and advanced tokenization method

Drawbacks:

- **Security in local phone system**: Cardholder’s information is stored locally in phone memory.
- **Compliance:** Sensitive data handling must be agreed upon by the issuers and vendors.

Today, cloud-based mobile payments are applied widely in several places, for example in refilling parking meter in San Francisco, car fueling and water service provision in East Africa. Its global competitiveness thanks to cloud technology can make a revolution in the mobile payment and telecom sector. Cloud-based mobile payment aims to set consistent mobile payment standard and creates strategic coordination across industries. (Emily 2018.)

2.3.7 Audio Signal Mobile Payment (NSDT)

As introduced by Instituto Economía Digital ESIC (2016), audio is a wireless element that can be exploited to make mobile payment. It is extremely useful for non chip-based devices and using acoustic features instead. Modern technologies such as Near Sound data transfer NSDT, Data Over Voice and NFC 2.0 are combined to produce audio signals that the microphone can pick up to create electronic transaction.

Audio signal mobile payment introduces some noticeable benefits over its drawback:

- **Security**: The server has entire control over the data to establish secure channel.
- **Low cost:** No extra hardware is required.

Drawback:

- **Noise interference** can affect the data transfer.

In the future, audio signal mobile payment can be a potential low-cost solution for m-commerce and will be put into use more widely.

2.4 Remote Mobile Payment

Remote payment does not require direct interaction with merchant's POS. Users can complete transaction globally, independently of consumer's or merchant's location. Remote payment is the essential and unavoidable payment method in the digital world as the demand of human beings. It enables people to make purchase or transfer funds without the physical distance. Moreover, security problem is handled very well in remote payment technology.

There are several remote payment methods, all of which are highly evaluated and adopted.

2.4.1 SMS-based Mobile Payment

This mobile payment is the simplest one that has been invented in 1997 by Coca Cola. The consumer can send a payment request via text message or an USSD to a short code and successfully made the purchase. The fee will be charged to their phone bill at the end of the month, reduce from prepaid balance or digital wallet. The merchant applied this method will be informed once the transaction is verified and release the goods.

This type of payment is based on MMS (Multi Messaging Service) technology. The difference between MMS and traditional SMS text-only is that MMS can deliver a variety of media content, ranging from image, video, audio, slideshow with much more capability.

The benefit of SMS-based transactional payment is that it is friendly-use for micropayment and does not require many technical steps. The process to end user is considered not complicated as the other methods. We can name a few advantages of this technology:

- Instant access to billions of mobile phone users globally
- No need to add or verify customers’ identity
- Customers do not need to provide information of their credit cards or bank accounts
- Billing is handled completely by the mobile phone carrier

However, there are some drawbacks that occurs while this technologgy is implemented:

- **Content adaption**: It is not always that the multimedia created by MMS is entirely compatible with the recipient’s mobile phone.
- **Bulk messaging**: Containing the media means that MMS will consume a large amount of bandwidth that can cause traffic over-the-air overhead.
- **Security**: The encryption of SMS/USSD is only provided until the radio interface, then the message is plain-text, which make it vulnerable to some security attacks.
- **Poor reliability**: Transactional SMS can easily fails as messages get lost
- **Slow speed:** Merchants take hours to receive the verification from recipient.
- **Low payout rate**: There are many high cost associated and operator estimate low payout rate, at about 30%.

During time, SMS-based Mobile Payment has gradually died out due to these severe limitations.

2.4.2 Mobile Banking

Mobile banking is not a new concept in the 2020s. At this time, most of all banking branches release their own mobile banking app, enable customers to keep track of personal financial status, money transfer, paying bills and all sorts of payment service. The wave started in certain countries like Sweden (Swish) and UK (Barclays) and has spread worldwide.

All banking institutions require a login procedure to verify customer's identity through the app. Once signed up, users are able to view their bank account and perform as many services as they would like in a convenient way.

Benefits:

- **Constant updates in customer experience**: The mobile app features will play a key role in new customer's adoption.
- **Convenience:** You can access your bank account anywhere along with your mobile phone.
- **Time-saving**: No need to book appointment or go to ATM to perform transactions.

However, there are still concerns about security issues within the bank software development team.

2.4.3 Mobile Web Payment (WAP)

There is a stereotype that affects people's understanding of mobile payment and mobile web payment. Mobile payment is when you use your digital wallet (Apple Pay or Android Pay) instead of your credit or debit card, to checkout in a physical location. Meanwhile, mobile web payment refers to payment that is made on browsers, or web app. It uses WAP (Wireless Application Protocol). This technology has some features that offer superior benefits compared to other payment types:

- **Enabling excellent customer service**: The web payment will provide predictable payment with quick interaction that can satisfy customer orientation.
- **Easy tracking:** The web pages always have a URL that helps customer to easily revisit the site or follow sales details.
- **Easy to use**: Customers are already familiar with web payment interface.

Mobile Web Payment is used widely in e-commerce, online shopping, booking tickets, etc. recently, mainly due to its convenience.

2.4.4 Direct Mobile Billing

The customer select mobile billing checkout at an e-commerce site. After two-factor authentication including PIN and One-Time-Password being provided, the purchase is made and the charge is applied to the customer's mobile bill. This kind of billing was most popular in 2012, when Ericsson and Western Union cooperated to release Western Union Mobile Money Transfers. Making use of its international advantages of both companies, the partnership aimed at building relationship between m-commerce and the financial market.

Direct mobile billing offered an improved service compared to Premium SMS-based billing, with some benefits listed down:

- **Security**: Threat protection and fraud prevention has been taken care of thanks to two-factor authentication engine.
- **Convenience**: No pre-installed or registration is required to proceed.
- **Speed:** Transactions can be complete within seconds.

The biggest drawbacks until now is the limit of value and type of goods that can be purchased.

2.5 Benefits and Drawbacks of Mobile Payment

After studying about various types of mobile payment, each with individual application and security technology, we can have a summary of comparison between the traditional payment and the mobile payment. The table below shows advantages and disadvantages regarding two payment systems respectively.

	Mobile Payment	Traditional Payment
Advantages	**Simplicity**: easy, friendly-use application	**Straightforward payment**: immediate, no device failure, errorless payment
	Convenience: No need to have separate cash, cards for risky pocket, now consumers can have all in one mobile phone.	**Security**: bank institutions are known to be highly secure in data protection
	Accessibility: Easy access to ready platform like smartphones	**High approach**: cash can be used in remote and less developed area
	Low cost: no extra cost as card-maintain fee	**No additional fee** service with cash
	Improve customer experience: The UX/UI design for mobile webs and applications are focused and tested to get better user's feedback.	
	Security measures are constantly added	
	Fast transactions within seconds	

	Loyal Customers: It is likely that customers will be loyal to bank institution and merchants that provides the most secure, smooth payment	

Although being considered as a favorable alternative to overcome the drawbacks of traditional payment, there are still controversies about digital wallet's security, compatibility, redundancy and adoption process.

	Mobile Payment	**Traditional Payment**
Disadvantages	**Investment cost**: High investment has been put in POS adapters, developing softwares, platforms, technologies.	**Additional processing fee** with credit card
	Security: Mobile phone is vulnerable for theft identity	**Counterfeit** cash is difficult to recognize
	Compatibility: older hardware devices are not compatible with newer technologies	Difficult to **keep track of**
	Phone failure: Your digital wallet may become useless in case of out of battery or no internet connection	**Inconvenience**: it is risky to bring your wallet or cash around
	Slow approach to old/less tech savvy and Third World users	

From the tables above, we can see that despite some minor disadvantages, mobile payment are an outstanding alternative to offer convenience, security and simplicity to make the purchase or perform financial transaction.

In the next chapter, we will have deeper research on the security mechanism that have been used in Mobile Wallet system and all security threats that can be found regarding all stakeholders in the Mobile Wallet ecosystem.

3 MOBILE WALLET SECURITY

In the tech-savvy era that we live in, security is the biggest concern regarding all services. As everything is provided in the form of digital, security becomes the critical weakness among other features, especially when it comes to payment. Therefore, the 3rd chapter includes deeper knowledge about various security features to be implemented in Mobile Wallet. Also, the research introduces common security threats to be analysed within the security threat model, involving all digital wallet stakeholders. From this section, we can have a brief overview of the Mobile Wallet ecosystem.

3.1 Problem Statement

Payment is a crucial area that security must be applied and taken throughout the entire process. Mobile users are, obviously, the fascinating target for stealing information. Attackers try to exploit those vulnerable security holes, perform identity theft, get access to sensitive data, make illegal changes to the bank’s database, and bring up uncountable loss to the financial state. We can name a few widely known case, when the weakness in security leads to enormous damage: Mobile payment security gaps exposed at Hong Kong university (Raymond 2017), Security Flaws at AT&T, T-Mobile and Sprint (Andrew 2018), Data breech exposed 1 million prepaid T-Mobile customers (PYMNTS 2019).

Along with the rapid growth and dominant of mobile development, a lot of research work has been invested to improve IT infrastructure in general and mobile application security in particular. The Information Technology field witnessed successful innovation, ranging in different services, especially in the digital wallet area.

As mobile payment is the communication between at least 2 devices, or even more, it is required that security must be implemented from both parties. Potential threats can lie in many parts of the payment processing process. Therefore, authorized entities give higher priority to be able to be confident in payment method. Some mechanisms come to life and are constantly applied in large scale, such as Password protected, PIN code, two-factor authentication, verification in each decision maker step to enhance the privacy of their customers. The focal point of the next section is the security technologies that are commonly used in mobile payment.

The most common technologies to be used in securing Mobile Wallet are authentication and cryptography. The next sections go through each of them in detail about their specific security mechanism.

3.2 Authentication

The first line of defense when it comes to security is authentication. Authentication is the act of verifying one's identity as who he or she claims to be, with one or two evidences (factors). (Vibha 2014.) It can be Single Factor (SFA) or Multi-Factor Authentication (MFA). The authentication factors can be categorized as the following:

- **User's knowledge**: something the users know, for example their PIN code, password, answer to profile information, etc.
- **User's physical characteristic**: something unique that can prove who the users are (biometrics), for example their fingerprints, face ID, etc.
- **User's possession**: something that only users have, for example, a security token, a key, etc.

People encounter many authentication challenges in their daily life, not only in mobile payment. Some easy examples include unlocking mobile phones, logging in to accounts in a website, withdrawing money from an ATM, ID registration, or just as simple as receiving a parcel.

Authentication accepts one’s credible proof of identity given by comparing the data inserted with their database. Once the authentication is successful, the user will be granted access to their service (can be personal account or digital wallet). The need of authentication rose from the past that many cite for the existence of password. Around the 1960s, an MIT researcher, later a professor, created a password to protect user’s file in a time-sharing file system. Since then, many techniques arose like Hash, public and private key cryptography (PKI), one-time password (OTP), CAPTCHAs, etc. Multi-factor authentication adoption started to take hold in the 2000s, when most of the authentication methods at that time were already bypassed by attackers. (Corey 2018.) In the scope of this thesis work, I only present some mechanisms that are considered to have significant effect on Mobile Wallet authentication.

3.2.1 One-time Password (OTP)

Passwords have been used for a few decades until 1980s, so have the technologies to bypass it. More and more digital system tools were leveraged to abuse passwords, even the longest passwords to be generated. A new authentication technique was just about the matter of time, and that is how One Time Password emerged. In 1984, to be exact, Security Dynamics Technologies, Inc. invented a methodology that produced one-time password with a time-based method from a special hardware device. (Emir & Mehmet 2019.)

The password can be generated by the following algorithms:

- Time-synchronization between the authentication server and client device
- A new password based on the previous password
- A new password based on a random counter challenge

The release of OTP solved the biggest problem of static passwords: they are immune to replay attack. Even if the attacker manages to get the password from another service or transaction, they are not able to login again with that expired OTP. OTP made a huge advantage to reduce attack surface. The payment system is not easily impersonated without the unpredictable data.

However, there are some limitations of OTP that might affect the whole system, according to Security Awareness 2019, including the following:

- No network connectivity makes it impossible to generate and validate OTP.
- OTP is sometimes difficult for people to memorize.
- It also requires other communication parties, for instance SMS messaging, which introduces some vulnerabilities to the payment security.
- OTP can be delivered with delay, or fails to deliver.
- It is costly for the provider.

Despite the above drawbacks, OTP is forecasted to gradually replace all static passwords to strengthen security systems due to its convenience (Gemalto 2020).

3.2.2 Tokenization

Tokenization is the process of replacing a piece of sensitive information by an equivalence that represents a unique sequence to a device. It is typically encountered as a numerical or alphabet chain that retains the critical data without compromising its security. It is very common to use tokens designated for a particular device, merchant or transaction. (Vibha R. 2014.)

The concept of tokenization has emerged long ago in the history, when people started thinking about how to secure and reduce risk of high value financial transactions. Payment Card Industry Data Security Standard (PCI DSS) has strict compliance of credit card data storing security. Therefore, tokenization met the requirement of PCI to protect the cardholder’s data.

Token service provider randomly generates the surrogate value that is converted from credit card information. In the case of payment card data, customer can insert the token to complete authorization request instead of the card number. Combining with NFC or EMV technology, the token is then stored in the merchant

POS system where it maps to the actual cardholder’s account in a secure tokenization system. The storage of tokens and payment card data is already complied with PCI and contains only the last 4 digits of the credit or debit card. By this way, Primary Account Number (PAN) is kept in secret and cannot be misused in other transactions with that particular POS merchant.

Tokens can be formatted in a variety of ways. In the context of payment system, there are 2 token types that differentiates in the length of value.

- **High-value tokens (HVT**) is used as an instrument, representing the actual PAN, that is able to complete the financial transaction automatically without the owner’s initiation step.
- **Low-value tokens (LVT)** or security token also acts as a sequence that match the actual PAN, but cannot complete the transaction by themselves, only with controlled context.

Tokenization is extremely effective to help:

- Strengthen authentication process, enhance payment system security
- Reduce the amount of data to be kept on hand
- Minimize the cost of compliance and ecommerce transaction

However, there are still some limits and risks in existence:

- Since token is quite simple and cheap, detokenization is easy to produce. Therefore, it is usually combined with PIN code or authorization code.
- Token is exposed to high risk if shared to other people or got stolen. Token must be kept safely and privately to prevent us from risky scenarios.

Tokens are implemented in almost all multi-factor authentication service, and will be put more into use in the future of authentication.

3.2.3 Biometrics

It is trendy to apply biometrics in authentication during the second half of 2010s. New devices and services can be easily seen to have biometrics integrated as a form of identity authentication and access control. Biometrics refers to measuring a person's unique physical traits and characteristics in personal identification. Biometrics is highly evaluated due to its distinction and reliability than other paper, document or ID techniques.

Biometrics consists of many approaches, which largely fall within 2 categories: physiological and behavioral. Physiological refers to body characteristics such as fingerprint, facial recognition, DNA while behavioral relates to people's behavior or movement measurement. Below are the most common biometrics technologies used in mobile payment to be listed:

- **Facial recognition**: is the process of identify or verify someone from a still digital image or video frame. In order to produce an accurate result, the facial recognition system compares facial features with the database. Face ID is more reliable and secure, especially with sensitive authentication such as initiating financial transactions. Face ID is now becoming the must-have technology in the latest smartphone models, starting from iPhone X (2017).

- **Fingerprint recognition:** Before Face ID, Fingerprint recognition has dominated the authentication system of smartphones with the name Touch ID. It is the figure that is recreated from friction ridges of the fingers. Fingerprint was already in use in banking industry, financial debt from the Feudatory of China. It is still used in recording identity or evidence in criminal crimes. In mobile payment system, fingerprint can be used to verify one's identification or transaction authorization request.

- **Retinal Recognition:** is a biometrics technique that scans through people's eyes. The pattern captures unique blood veins of each individual and authenticate. The idea of Retinal Recognition was first introduced in

1935 by Dr Carleton Simon and Dr Isadore Goldstein from New York. 44 years later in 1981, the initial model was brought to life. (The Gale Group 2014.)

- **Signature Recognition**: can authenticate users by their unique handwriting style. It compares the signature characteristics given with the sample one from database.

- **Voice Recognition:** The acoustics features of the voice are recorded and translated in the speaker recognition system to distinguish individuals. Voice recognition is applied in device intelligent assistant, translation, making phone call, payment transaction.

Biometrics increases the authentication security, provide convenient checkout option for consumers, and reduce fraud significantly. However, developers must constantly improve and enlarge biometrics database for achieving accurate decisions.

3.3 Cryptography

Along with authentication, cryptography is the essential security features that is needed to protect and secure information. Data security must be enhanced throughout the payment system, including storing in database and transferring between any channels.

Cryptography consists of encryption and decryption. Encryption is the procedure of encoding the plain text message using cipher algorithm. The purpose of encryption is to make changes to the data so that it cannot be read or heard normally except for the authorized parties. Decryption will convert the ciphertext back to plaintext. Both encryption and decryption involve a secret element called key as described in the figure 3 below. The key can only be obtained by authorized users to encrypt or decrypt the message. (Emir 2017.)

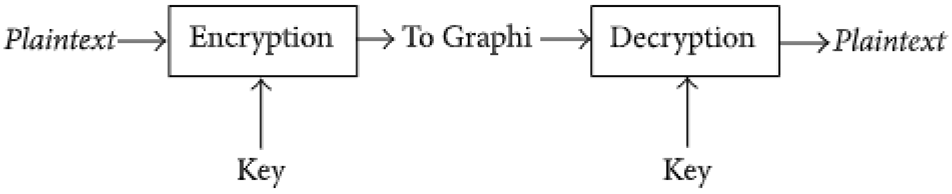


Figure 3. Encryption Process (Emir 2017)

Depending on the key type, there are 2 types of encryption algorithm.

3.3.1 Symmetric Encryption

Symmetric Encryption, or Private Key Encryption is the algorithm when the same key is used for both encryption and decryption. The usual length of symmetric key is less than 128 bits. The key is created by pseudo random generator (as random as possible) to ensure best security. Since the keys are identical, they should always be a shared secret between all parties. Otherwise anyone receiving the key would be able to decrypt the private message.

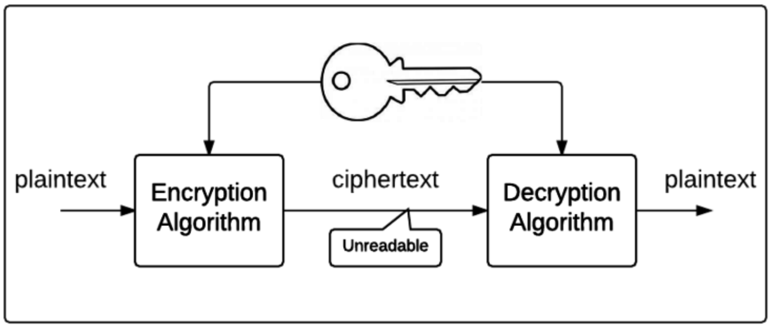


Figure 4. Symmetric Encryption (Emir 2017)

Symmetric key can be stream ciphers or block ciphers. Stream ciphers process data at one bit/byte at a time, meanwhile block ciphers process data in data blocks. We will focus on block ciphers in relation to mobile payment.

DES

Data Encryption Standard (DES) was developed by IBM in the 1970s but was later adopted by NIST. It has a 64-byte block size and use a 56-bit key to generate the encrypted message. DES is vulnerable to brute force attack if a weak, short key is used. It is already publicly broken in 22 hours and 15 minutes by EFF in 1999. (Paul 2001.)

3DES

3DES is an implementation of DES to prevent feasible brute force attack. 3DES applies 3 DES algorithms in each block, numbering encryption with key 0,1 and 2. 3DES triples the key size of DES to protect against attacks, without changing the block algorithm.

AES

One of the most common standards for Symmetric Encryption and successor of DES is Advanced Encryption Standard (AES). It was originally developed by Joan Daemen and Vincent Rijmen in 1988. In 2001, National Institute of Standards and Technology (NIST) officially approved AES in commercial (Federal Information 2001). AES supports many combinations, including AES-128, AES-192, and AES-256 (according to the bits key length). AES utilized the 4x4 matrix with many cell (each contains 1 byte) forming a block (16 bytes). AES is considered as almost unbreakable, large enough data block and recommended to use.

3.3.2 Asymmetric Encryption

Asymmetric Encryption, or Public Key Encryption uses 2 different keys for encryption and decryption as described in figure 5. It was described by Diffie and Hellman in 1973. Afterwards, Asymmetric key is now widely used and also known as Diffie-Hellman key exchange.

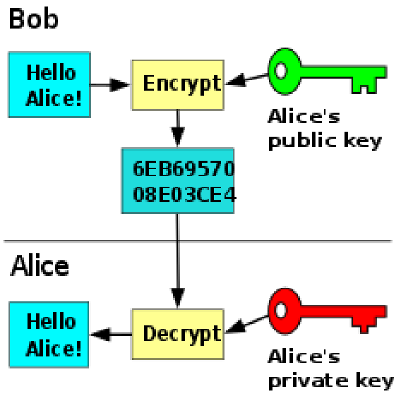


Figure 5. Public-key Cryptography (Tutorials Point)

The recipient's public key is established to encrypt the message, but only the receiving parties who possess their private key is able to read the encrypted message. They key generation contains mathematical calculations so that one key cannot used to predict the other one. This one-way function ensures the confidentiality, as only the owner of the private key and associate who has public key are involved.

RSA

RSA (Rivest–Shamir–Adleman) is a widely applied public key cryptosystem in securing data transmission. It is invented in 1977 and named after its three inventors. RSA is one of the first and best known for public key data block encryption.

RSA is based in the factorization of 2 prime numbers to generate the public and private keys, ranging from 1024 to 4096 bits. The sender encrypts the message with the recipient's public key, and only the private receiver's key can decode the message.

RSA contains many vulnerabilities. A small value of 2 prime numbers will produce a too weak key encryption process. It is possible for attackers perform probability attack. On the other hand, large value will consume a lot of time and effort compared to other encryption mechanisms. Due to many flaws in its algorithm, RSA is not directly applied in cryptography, but combined with symmetric encrypted shared key to increase the complexity and security of bulk encryption-decryption level.

Public Key Infrastructure

Public Key Infrastructure (PKI) is not a specific technology but refers to a set of roles, policies, procedures that is created to maintain the use of Public Key Encryption. The primary purpose of PKI is to secure data transmission via network such as e commerce, internet banking, confidential email.

PKI was developed by Government Communications Headquarters (GCHQ) in the 1970s PKI binds the public key with respective identities. Examining the diagram below, we see that:

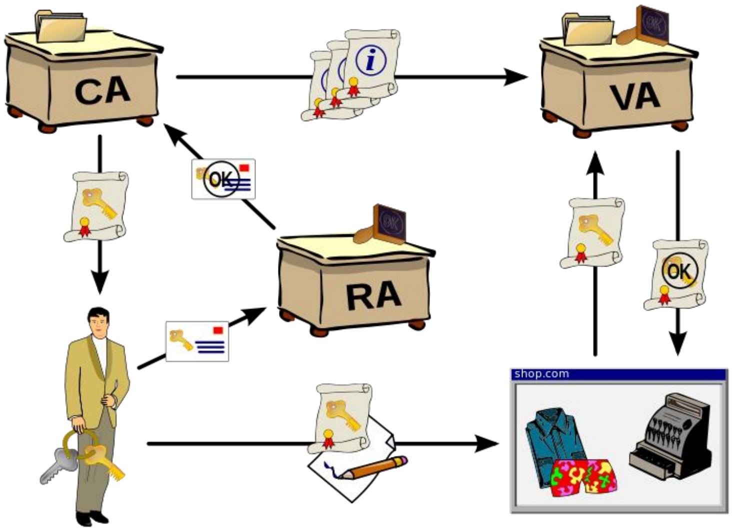


Figure 6. Public Key Infrastructure (Tutorials Point)

- **Certificate Authority (CA)** establishes the lifecycle of registration and issues the certificate.
- **Registration Authority (RA)** assures the validity and correction of the registration of digital certificates and requests.
- **Validity Authority (VA)** provides service to verify the validity of a digital certificate.

PKI applications go beyond user ID and authentication, but also Digital Signature, Digital Certificate, SSL/TLS, etc. PKI makes a big contribution by supporting authentication in smartphone, game console, ticketing, mobile banking in particular and e-commerce in general.

Hash Function

Hash Function is also Public key cryptography. Hash function is a mathematical calculation that converts the input data (Key) into a fixed-length hash code. The input can have variable sizes but Hash Function always produce a fixed-size value, indexing a hash table or records. Since the hash is usually much smaller than the input data, it is also known as digest. (Tutorials Point.)

Hash function is extremely reliable and entrusted directly in Password Storage and Data Integrity Check. It is popular among many web and mobile protocols.

The effectiveness of Hash function is measured by 2 criteria:

- Hash code does not take long to output
- Duplicate values should be removed

There are some popular Hash Functions that is widely used currently.

Message Digest (MD5)

Message Digest (version 5) was largely used for quite some time. It generates the 128-bit hash code. It was created by Ronald Rivest in 1991 and later adopted as Internet Standard RFC 1321. (Mark 2009.) MD5 is widely implemented in pre-computed data integrity check, mostly in file server, until 2004 when continuous collisions are found. MD5 is no longer recommended for use after being attacked in only an hour by a cluster.

Secure Hash Algorithm (SHA)

Secure Hash Algorithm is a family of cryptography that is published by NIST in 1993. SHA calculates and represent a condense message. If the input message is less than 264 bits, SHA will produce a 160-bit length message.

SHA-1 has been widely imported in security applications and protocols, for example in Secure Socket Layer (SSL). Throughout the time, NIST released SHA-2 and SHA-3 with extended input length.

Whirlpool

Whirlpool is the latest Hash Function cryptographic system. It was first introduced in 2000 by Vincent Rijmen, creator of AES. Whirlpool returns 512-bit hash message, which is an improvement in data length. Until now, 3 versions of Whirlpool have been released, namely WHIRLPOOL-0, WHIRLPOOL-T, and WHIRLPOOL. It is likely that Whirlpool will be more common in the near future of Hash Function.

The biggest threat to cryptography is the brute force attack, where the hackers try to input all possible key combination. The length of the key is exponentially proportional to the strength of the encryption. Thanks to advanced technology nowadays, the more complex the encryption, the more secure it is, probably taking a few billion years to decrypt the message.

Cryptography is utilized in many data systems. Cryptography is commonly used both for data at rest, such as in storing devices, drives, portable devices, and records. It is also used at transit for transferring data via network (the Internet, e-commerce, mobile platform, wireless communication, ATM, etc.)

3.4 Security Threat Model and Element

Mobile payment with digital wallet is a large ecosystem that consists many stakeholders. In order to maintain the function of any system, the ecosystem must include parties that take part in all activities, from the beginning till the end. Each stakeholder is a basic component of the mobile payment system and plays an irreplaceable role during the transaction. They are identified as the following diagram (ENISA 2016):

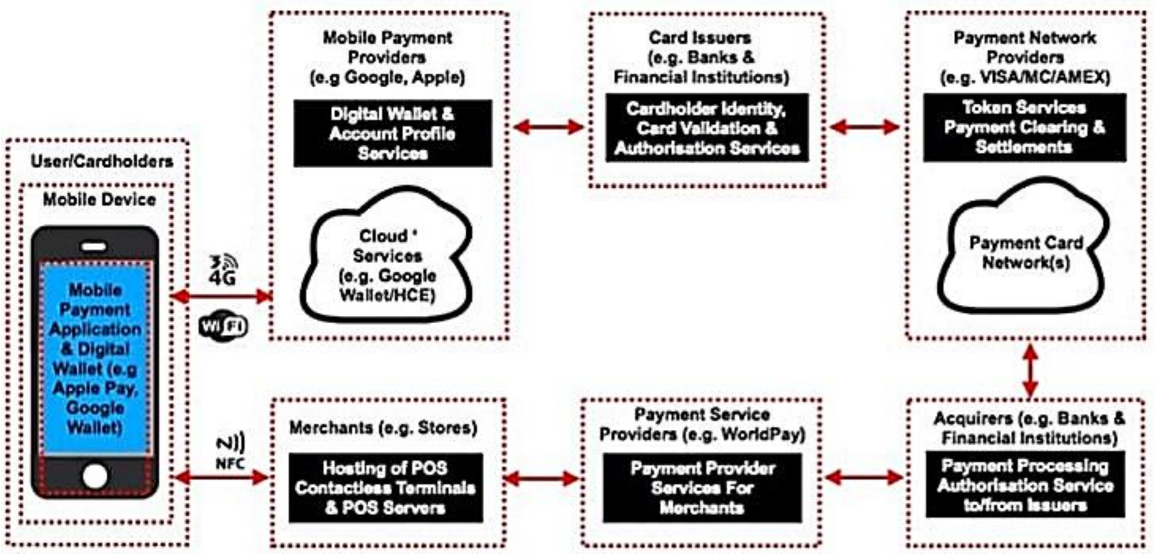

Mobile Payment Providers (e.g Google, Apple)
Digital Wallet & Account Profile Services
Cloud * Services (e.g. Google Wallet/HCE)
Card Issuers (e.g. Banks & Financial Institutions)
Cardholder Identity, Card Validation & Authorisation Services
Payment Network Providers (e.g. VISA/MC/AMEX)
Token Services Payment Clearing & Settlements
Payment Card Network(s)
User/Cardholders
Mobile Device
Mobile Payment Application & Digital Wallet (e.g Apple Pay, Google Wallet)
3G
4G
Wi Fi
NFC
Merchants (e.g. Stores)
Hosting of POS Contactless Terminals & POS Servers
Payment Service Providers (e.g. WorldPay)
Payment Provider Services For Merchants
Acquirers (e.g. Banks & Financial Institutions)
Payment Processing Authorisation Service to/from Issuers

Figure 7. Digital Wallet Ecosystem (ENISA 2016)

3.4.1 Digital Wallet Stakeholder

The above stakeholders are introduced as below (European Payments Council 2014):

User/Cardholder: Customer is the critical element of mobile payment system. He/she is the owner of the bank account, the mobile device and is the one who initiates the mobile transaction. The customer is the key factor of mobile payment success, who evaluates the customer experience, customer service, controls the type of digital wallet he/she wants to use, and makes necessary arrangements with the issuers and service providers.

Mobile Payment Provider: This stakeholder provides the application and infrastructure of the digital wallet. Major players in the market includes Apple Pay, Google Pay, Samsung Pay, Alipay, WeChat, etc. Users can make the purchase via these applications with their cardholder’s information in the app.

Card issuer: The bank and financial institutions are corporations that offers banking and financial services such as open a bank account, issue personal card payment, validate card data, authorize and complete transactions, partner with payment service providers, etc.

Payment Network Provider: Payment Network is the party that implement payment card network, tokenization service, payment clearing and settlements. The example of Payment Network Provider is VISA, MC, AMEX.

Card Acquirer: The banks and financial institutions also provides card payment processing, authorization to/from the Issuer.

Payment Service Provider: is the stakeholder that provider payment service for merchants to serve digital wallet payment within POS's terminal, like WorldPay, etc.

Merchant: is the party that offers and sells products or services directly to the customers. Customers will make the purchase with this party. Merchant is the host of POS terminal.

3.4.2 Secure Electronic Transaction (SET)

Secure Electronic Transaction is a protocol specified for credit card transactions via Internet. SET is developed by partnership between Visa and MasterCard, with the help of cryptology companies like Microsoft, IBM, RSA, VeriSign. It is implemented to maintain security during the transaction flow. (Vibha 2014.)

SET also enhances the security in mobile payment (Saleem & Muhammad 2007), including

- Authentication
- Authorization
- Confidentiality
- Integrity
- Non-repudiation

SET is also defined as the following process:

1. Consumers access the merchant’s web site, browse the goods and selects what they want. They will get the total cost of all chosen items including taxes and shipping costs.
2. Consumers choose the payment method to proceed with
3. After getting details of customer’s payment, the merchant contacts the merchants bank for customer authorization
4. Merchant Bank will contact the customer’s bank to get payment approval
5. The transaction will be complete if authorization is correctly conducted
6. A few seconds later, there is a confirmation to the customer that this order has been processed.

Maintaining a SET mobile payment process is the top criteria in developing digital wallet application.

3.5 Security measures

The table below shows the most common security threats and the prevention from each stakeholder’s perspective (ENSA 2016):

Mobile Payment Stakeholder	***Potential Threat***	***Security Measures***
User	**Phishing:** • Public Wi-Fi network • Media attachment	• Security awareness • Keep phone updated • Do not use public Wi-Fi for mobile payment
Mobile device	**Unauthorized access control:** Weak PIN	• Strong PIN • Biometrics authentication factors: face ID, fingerprint, etc.

	Data interception via spyware installation: • Outdated OS • Untrusted source app installation • Jailbroken device • Zero-day vulnerabilities	• Keep OS updated • Maintain default security features and settings • Do not download apps or open files from suspicious sources
Mobile Payment Application	**Exploited vulnerabilities:** • Credit card provisioning: stolen card misused, raw images contain sensitive data • API vulnerabilities • Weaknesses in pairing with other hardware devices (AirPod, Smartwatch) • Brute force attack due to weak PIN	• Insecure connection with POS terminal • Insecure token in MST connection • Inadequate signal strength in MST • Periodically performing tests and validation for software application securities
	Reverse engineering source code	• Secure coding practices • Jailbreak detection • Anti-debugging • Source code obfuscation
Merchant	**Potential malware** in POS terminals due to using default password, POS misconfigurations, patching systems	• Change default POS password • Keep POS updated
	Relay attack from insecure LAN access and lack of enforcement of privileges for POI and POS access	• Deploy and configure firewall • Restrict POI and POS access to authorized users

	MiTM attack: insecure connection between POI and POS	SSL configuration for POI and POS
Financial institution	Weak access control to critical database while mobile device has all cardholder’s details	Enforce strong multifactor authentication and privileges for critical database
	Payment fraud, token compromise, malware	Deploy effective fraud management rules and malware detection with log analysis
Payment Service Provider	Software flaws and vulnerabilities in POI and POS	Ensure design-flawless software, security testing between POI and payment gateway hosted at Payment Service Provider
	Data connectivity	Ensure secure, encrypted point to point (PTP) connection between merchant POS and PSP, PSP and acquirers
Mobile network Operator	Untrusted SMS message	Provide encrypted communication channel
Mobile Payment Application Provider in Server and Cloud System	Cardholder’s data privacy compromise	Issue security policies regarding data protection
	Malware in server	• Deploy malware detection and prevention measures • Enforce 2FA for critical server access • Enforce access privileges
	Stolen card enrollment Fraud payment transaction	Implement fraud detection against stolen card’s registration and payment transactions

	Denial of Service (DoS) attack	Implement anti DoS measures in critical server and cloud service

We can detect the security threats that might be exploited from the table above and follow the security measures to avoid exposing security holes and vulnerabilities to attackers. This can be applied for users, mobile application developer, merchant, Payment Service Provider, etc.

4 CASE STUDY OF MOMO

In the market of Mobile Wallet in Vietnam, MOMO overcomes many formidable opponents from big corporations like Apple Pay and Samsung Pay as an undisputable leader to gain more than 13 million users (as of 2020) and nowadays plays a significant role in the mobile payment industry. It is renowned for quick and reliable payment. By focusing on their security improvement, MOMO successfully gains the trust of many mobile users. MOMO is proud to be the first tech company in Vietnam receiving PCI DSS (Payment Card Industry Data Security Standard) with the highest level for service provider.

4.1 MOMO overview

Following MOMO website, MOMO is an e-wallet and payment app that allows users to make purchases online and transfer money digitally in various platforms: POS, Desktop, Website and Pay in bill. MOMO offers various services, including nationwide cash transfer, support more than 100 types of bill charges, recharge mobile phone bills, pay personal loans, purchasing software licenses, online game cards, taxi payments, flight and movie tickets. The figure below shows the picture of e-commerce payment method used in Vietnam.

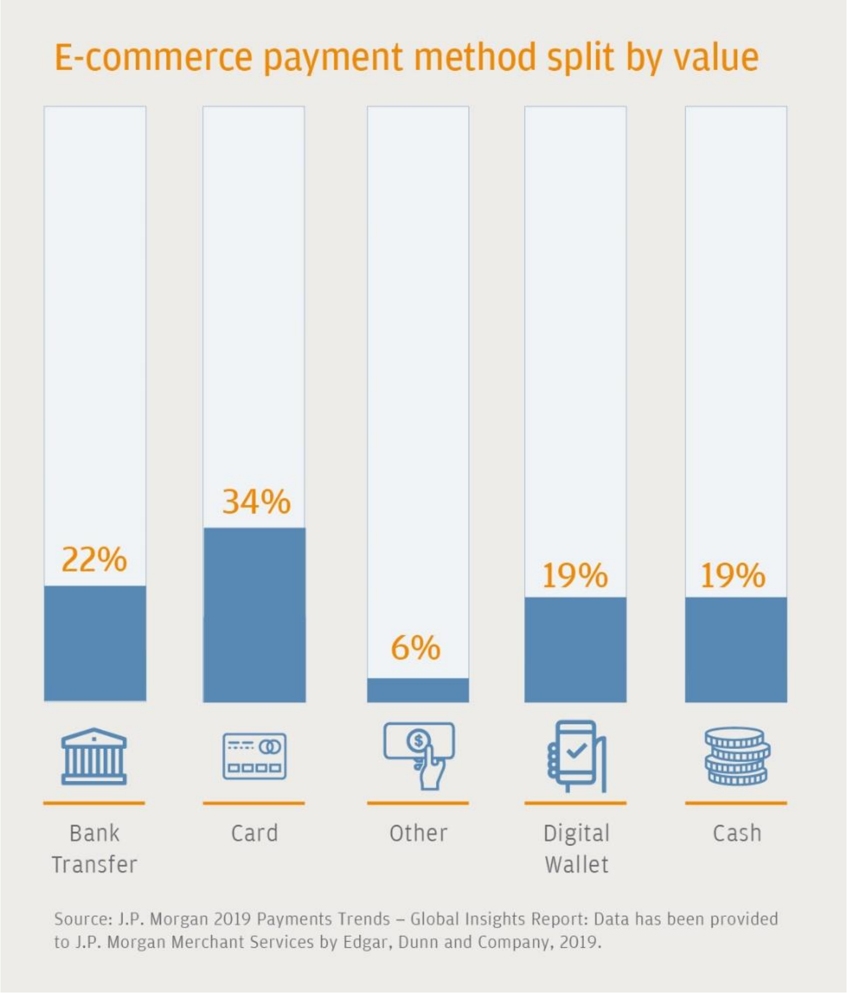


Figure 8. Vietnam E-Commerce Payment Method 2019 (J.P.Morgan)

Apparently, digital wallet is slowly adopted (19% of the total value) in Vietnam and has the tendency to be preferred among others.

From MOMO website, MOMO developed from a Fintech startup company that develops digital wallet application for iOS and Android devices in 2007. Following the affluent success of giant Asian tech companies like Tencent’s WeChat, Indonesia’s Go-Jek and Singapore’s Grab, MOMO has risen to become a notable mobile payment service provider. The company partners with 24 domestic banks and major foreign payment organizations like Standard Chartered, JCB, MasterCard and Visa. There is estimated to be about 10 000 merchants in diverse fields such as e-commerce, transportation, entertainment, utility, consumer shopping in cooperation with MOMO. Some achievements to be listed that MOMO team has successfully gained throughout the time, such as the following:

- Highest rank software application in Apple Store Vietnam (two times) (2019)
- Top FinTech100 according to KMPG 2018
- Top 3 financial application for Android 2014
- Best Mobile Product of The Year 2012, 2013, 2014

MOMO is highly appreciated by mobile users (highest percentage in Vietnam's market share in Figure 9) in terms of its security and UI/UX design. Under the circumstances that nearly 80% of Vietnamese population do not have a bank account, cash handling is dominating the financial market, and people who want to use e-wallet would anyway be affordable to use and choose Apple Wallet or Samsung Pay, MOMO still proves to be the remarkable expert in the long run. It is called the most favorite Vietnam e-wallet.

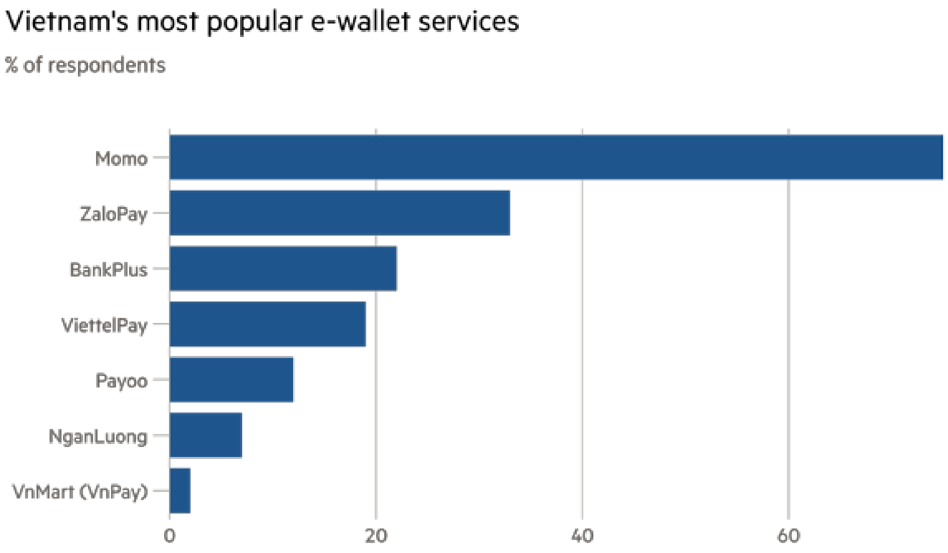


Figure 9. Vietnam's most popular e-wallet 2019 (FT Confidential Research)

What sets it aside from other applications from any banks is that they acquire users with nonstop development for the best customer experience (UX design). The company's vision is to make a revolution promoting cashless payment in

Vietnam. Though ambitious, there are many persuasive evidences that MOMO can make it happen in the near future. (Fintechnews Vietnam 2019.)

4.2 MOMO Security Mechanism

MOMO commits to Mobile Money Security of State Bank of Vietnam (SBV) under the act of Decree 101/2012, General financial services, Bank regulator and Global System for Mobile Communications (GSMA) Association (Asia Tech Daily 2019). MOMO dedicates to try their best implement the Mobile money security system and ensure user's data privacy. R&D team at MOMO invest much time and expense to deliver most updated high secure technology. This factor has an enormous impact in attracting new app adopters and maintaining MOMO's good reputation. Users can be ease to know that MOMO are applying many outstanding and superior security technologies (MOMO security website), which are thoroughly introduced and evaluated in the next session.

4.2.1 Two-factor Authentication (2FA)

As described above in section 3.2.1, multi-factor authentication is crucial to any mobile payment system, especially in digital wallet. Among all authentication types, two-factor authentication (2FA) is the most popular security mechanism to be used, ranging from many different services, in authentication, verification and confirmation steps. MOMO also requires 2-step authentication simultaneously to get personal identification.

Users must provide user-defined information (for example password, PIN) and information that users receive from the service provider (OTP, Token, Grid card) in order to complete their requests. The OTP code is sent via SMS to your MOMO Wallet registration phone number. 2FA applies when users register a new account or device, log in and complete a financial transaction. To tighten the security level, MOMO enables warnings against any irregular or suspicious logins, activities and transactions.

With two factors combined algorithm, hackers will not able to fully steal the information needed to penetrate the user account, therefore increases the security level. Moreover, MOMO also integrates modern biometrics authentication such as Fingerprint and Face Recognition to authenticate users.

4.2.2 Tokenization

Tokenization is a security solution that major credit and financial institutions have applied when issuing payment cards to their customers. It is already mentioned in section 3.2.2 that tokenization is a technology which automatically encrypts the cardholder’s details into token code. Instead of storing the customer’s payment card data, only the token is recorded in the system.

By this way, data privacy is protected against data breach. Attackers are not able to access the actual card data since token is only valid for a particular transaction only and cannot be used out of this scope.

4.2.3 Digital Signature

Digital signature mechanism is explained in section 3.3.2. It is an asymmetric cryptography that provide security and validity for the message.

MOMO uses HMAC_SHA256 algorithm to generate signature. (Developers MOMO Docs, 2019). Input data includes Secret Key and data, data generated with format: key1=value1&key2=value2... The code below shows a sample request that inclues data about access key, partner code, request type, order ID, order message, amount of money, etc. to be encrypted with HMAC_SHA256.

key1: field name, value1 = value of key1

```
{
  "accessKey": "F8BBA842ECF85",
  "partnerCode": "MOMO",
  "requestType": "captureMoMoWallet",
  "notifyUrl": "https://momo.vn",
  "returnUrl": "https://momo.vn",
  "orderId": "MM1540456472575",
  "amount": "150000",
  "orderInfo": "SDK team.",
  "requestId": "MM1540456472575",
  "extraData": "email=abc@gmail.com",
  "signature":
"996ed81d68a1b05c99516835e404b2d0146d9b12fbcecbf80c7e51df51cac85e"
}
```

How to create Digital Signature:

```
partnerCode=$partnerCode&accessKey=$accessKey&requestId=$requestId&amoun
t=$amount&orderId=$orderId&orderInfo=$orderInfo
&returnUrl=$returnUrl&notifyUrl=$notifyUrl&extraData=$extraData
```

Data Processing:

```
partnerCode=MOMO&accessKey=F8BBA842ECF85&requestId=MM1540456472575&amoun
t=150000&orderId=MM1540456472575&orderInfo=SDK
team.&returnUrl=https://momo.vn&notifyUrl=https://momo.vn&extraData=emai
l=abc@gmail.com
Secret Key: K951B6PE1waDMi640xX08PD3vg6EkVlz
var signature = HmacSHA256(data, secretkey);
console.log(signature);
```

4.2.4 RSA Encryption

RSA Encryption is introduced in section 3.2.2.2. RSA uses a public key and private key to encrypt and decrypt the data while transmitting. Partner uses public key provided by MOMO to encrypt the data in MOMO's format, MOMO uses private key to decrypt (Developers MOMO Docs 2019). Below is an example of data encryption by RSA in MOMO service.

Data before encrypt RSA

```
{
  "partnerCode": "MOMOIQA420180417",
  "partnerRefId": "Merchant123556666",
  "partnerTransId": "8374736463",
  "amount": 40000,
  "description": "Thanh toan momo" (means MOMO payment)
}
```

Data after encrypt RSA

```
A7WFmmnpn6TRX42Akh/iC5DdU5hhBT9LR5QSG6rJAl70hfEkkGUx2pTCai8s+M9KMVUcJ7m5
2iv74yhmeEjjN10TtEJoqITBIYBG2bqcTprhDijyhV4ePU7ytDNuLxzzIvGfTYyvbsEJ2jZT
Sf556yod12vhYqOJSFL/U2hVuxjUahf5Rnu5R/OLalg8QmlU6nQooEuNdzEXPMd6j9EaxOCi
B2oM5/9QiTN0tCNSTIVvPtnlHu5mIbBHChcwfToIL4IAiD1nbrlDuBX//CZcrZj6hFqjvU31
yb/DuG02c3aqWxbZKZ8csOwF9bL30m/yGr/0BQUWgunpDPrmCosf9A==
996ed81d68a1b05c99516835e404b2d0146d9b12fbcecbf80c7e51df51cac85e
```

4.2.5 SSL/TLS

SSL (Secure Socket Layer) and TLS (Transport Layer Security) are cryptographic protocols that aim at protecting data transmission via networks (such as the Internet). SSL/TLS ensures the communication security for connections between a client (web browser) and a web server:

- SSL/TLS encrypts the transmitted message so that the connection is secure and private. It is a symmetric encryption that keys are generated uniquely in each session (TLS handshake protocol).
- Data integrity is ensured as SSL/TLS uses a message authentication code and make the connection becomes reliable.
- The identity of each parties is identified using public key cryptography.
- SSL/TLS is working on top of some reliable transport protocol (TCP) in OSI model (Dierks & Rescorla 2008). TLS is the successor of SSL and solves many SSL's vulnerabilities. Nowadays, SSL/TLS certificate is considered one of the basic global technology security standards for data transfer in server configuration.

MOMO's SSL/TLS data transmission encryption technology has been certified by the world's leading international security company GlobalSign. GlobalSign is a Webtrust-certified certificate authority (CA). In 2012, GlobalSign launched an online service that allow Web administrators to certify that they have correctly configured SSL across their website against any faulty and exploitable SSL configurations. GlobalSign certificate shows that MOMO security level is highly entrusted.

4.2.6 MOMO Payment Platform API

MOMO Payment Platform API is a payment solution for business units, allowing customers to use MOMO E-Wallet account to pay for services on various platforms: Desktop Website, Mobile Website, Mobile Application, POS, Pay In Bill, In App MoMo (Developers MOMO Docs, 2019).

There are 4 primary payment methods that MOMO supports: Payment Gateway (All-in-one), App-In-App Payment, POS Payment, QR Code Payment. Each payment method uses separate API platform.

- Step 1: Customer checks order and selects MOMO as the payment method.
- Step 2: Your server creates a payment session and sends payment request to MOMO.
- Step 3: Redirect sales page to MOMO’s payment page.
- Step 4,5,6: Customer uses MOMO app to scan QR code or Login to make payment.
- Step 7: After payment, MOMO redirects customer to the sales page.
- Step 8,9: Your server confirms the transaction and updates services for User.

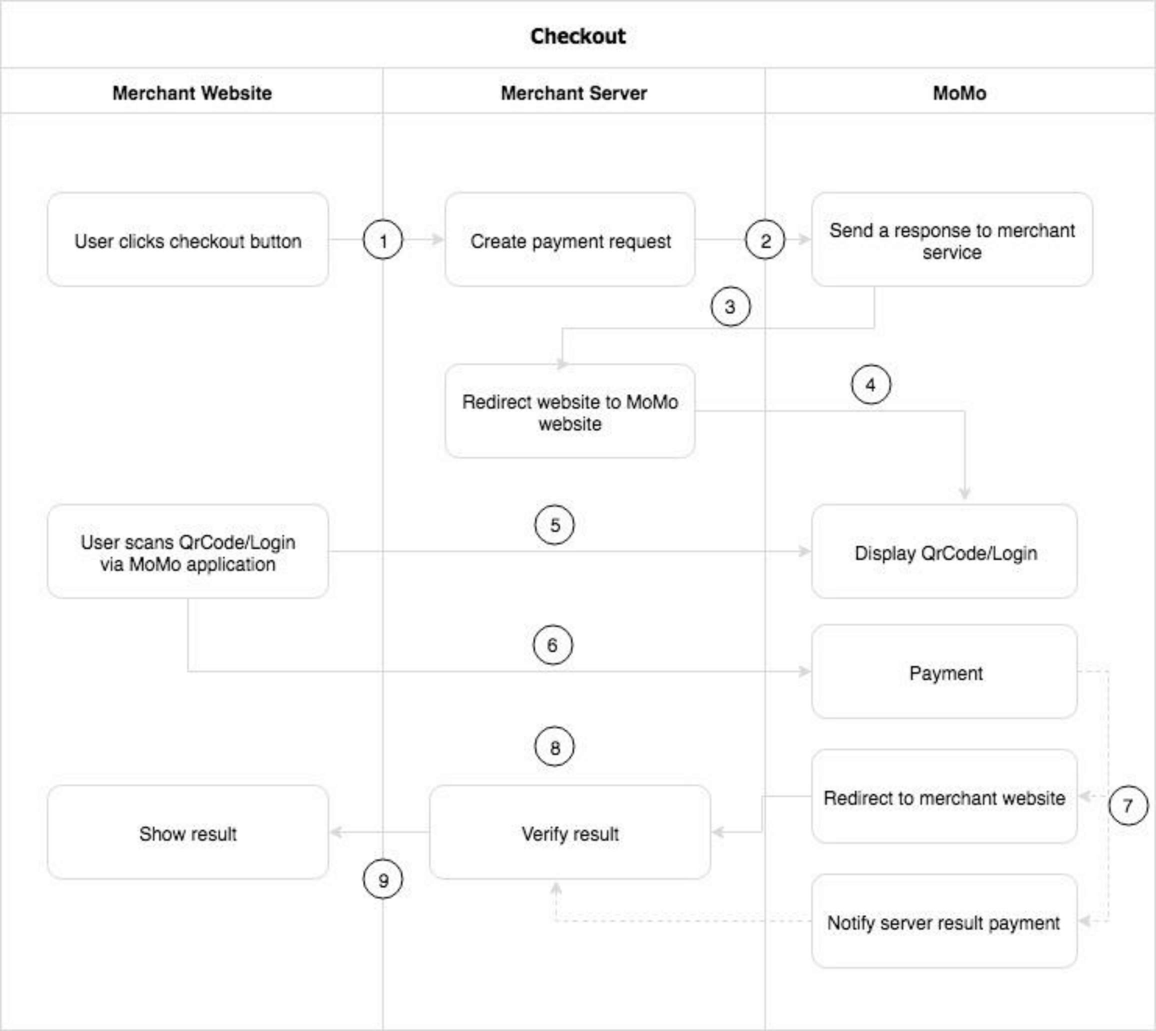

Checkout
Merchant Website
Merchant Server
MoMo
User clicks checkout button
1
Create payment request
2
Send a response to merchant service
3
Redirect website to MoMo website
4
User scans QrCode/Login via MoMo application
5
Display QrCode/Login
6
Payment
7
8
Redirect to merchant website
Show result
Verify result
9
Notify server result payment

Figure 10. Payment on Website Desktop / Mobile MOMO (developers.momo.vn)

4.3 Security Testing Guidelines

We go through the theoretical part about MOMO security system in the previous section. In order to analyze and examine the security technologies mentioned above, I will perform the practical part using different frameworks and network analysis tools.

After researching, I have decided to take OWASP as reference for laying issue foundation. OWASP is a standard awareness documentation for developers and web application security. OWASP aims to improve software security through its community-based sharing knowledge, open source projects, material related and tens of thousands of members. OWASP guidelines present the top security criteria that are most concerned. By adopting this documentation, companies and developers can build a more secure application and minimize security risks. (OWASP Top Ten 2020.)

A security testing experiment will be made based on OWASP, shortly described as the table below.

The top 10 Web Application Security Risks:

Security Threats		**Information**
1	***Improper Platform Usage***	This security category includes the misuse of a platform feature or failure to use platform security controls, for example: • Violation of published guidelines: refers to mobile applications that contradict the best practices recommended by device's platform (iOS, Android, Windows intents) • Unintentional misuse: insecure coding leads to exposed service or API call
2	***Insecure Data Storage***	This security threat is detected when data can be attained from a lost/stolen mobile device or a malware that can execute on behalf of the device. Insecure data storage may result in identity theft, privacy violation, SQL injection
3	***Insecure Communication***	Insecure communication is all the security threats that are related to the data exchange between client-server over the network, for instance Wi-Fi, NFC, Bluetooth, SSL/TLS, TCP
4	***Insecure Authentication***	Insecure Authentication contains all the threats regarding authentication, session management, password policy, tokenization, POST/GET request, etc.
5	***Insufficient Cryptography***	Broken cryptography can bring in data leakage, information theft, etc. Insecure encryption algorithms such as RC2, MD4, SHA1 should be avoided

6	***Insecure Authorization***	If an organization fails to authenticate an individual before executing an API endpoint requested from a mobile device, then the code automatically suffers from insecure authorization
7	***Client Code Quality***	Poor code quality vulnerability can lead to high risk drive-by Jailbreak attacks. Poor code-quality issues (such as Buffer Overflow) are typically exploited via malware or phishing scams
8	***Code Tampering***	Typically, an attacker will do the following things to exploit this category: • Make direct binary changes to the application package’s core binary • Make direct binary changes to the resources within the applicaiton’s package • Redirect or replace system APIs to intercept and execute foreign code that is malicious
9	***Reverse Engineering***	An attacker may exploit reverse engineering to achieve any of the following: • Reveal information about back end servers • Reveal cryptographic constants and ciphers • Steal intellectual property • Perform attacks against back end systems • Gain intelligence needed to perform subsequent code modification
10	***Extraneous Functionality***	Typically, an attacker seeks to understand extraneous functionality within a mobile app in order to discover hidden functionality in in backend systems. The attacker will typically exploit extraneous functionality directly from their own systems without any involvement by end-users

5 SECURITY TESTING IN MOMO

The security testing will be conducted using many techniques and security frameworks to evaluate the effectiveness of security features that are implemented in MOMO Mobile Wallet. Following the security guidelines defined from OWASP Top 10, we can check and assure that the best security practices are applied.

The security tests are presented with specific aim, category, preparation needed, the experiment conducted and conclusion from the result. Although the tests do not cover all security threats as in the guidelines, it contains some tests that can check common security holes that can directly do harm to the end users.

5.1 Intercepting NFC communication in order to gather credit card information of the consumer

The aim of this test is to check if the NFC tag identifier is encrypted so that the transaction process is secure (Related to the 3rd threat).

The test requires two Android smartphones, one is installed with MOMO, the other one is installed with an NFC Reader application.

The experiment is done with two different devices. One serves as the customer's own device with MOMO wallet installed. The other one acts as the hacker's phone without MOMO application. A payment code is generated on the customer's phone that will carry information for payment as if the customer is at the counter. However, the attacker's smartphone could not read the payment code with a normal NFC reader due to the lack of unknown tag identifier. The transaction was not processed (see Figure 11 below).

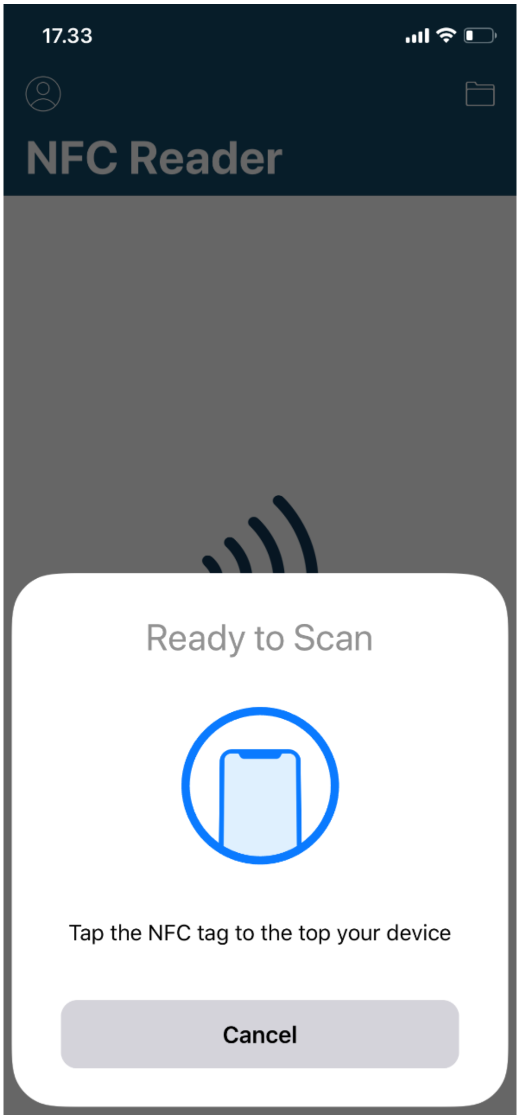


Figure 11. NFC Reader trying to read MOMO payment's code

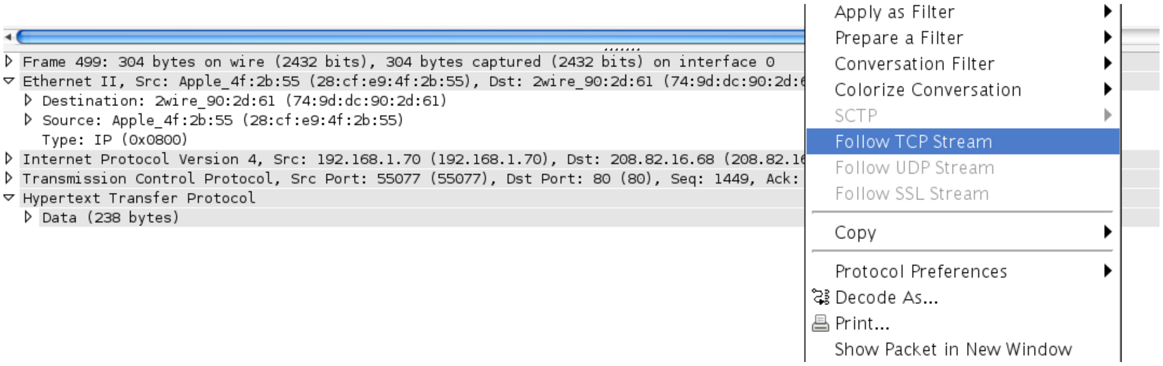
The conclusion was that this security test proved NFC communication cannot not be intercepted to steal credit card information from the customer's mobile wallet.

5.2 Intercepting communication of the mobile application

The aim of this test is to use a network protocol analyzer to monitor packets going through the application, in order to inspect the security level of the software (Related to the 3rd threat).

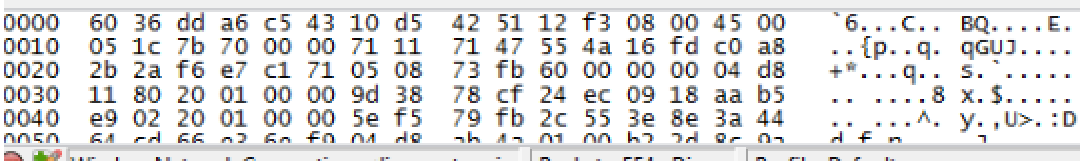
The test requires an Android smartphone device, Wireshark software to run on the computer, Packet Sniffer application (a software designed specifically for monitoring and capturing packet on an Android device, the same as Wireshark). When working with Wireshark, the steps to be carried out are as below:

- Install Wireshark to the computer. Download Android SDK emulator for testing.
- Start the Android Virtual Device (ADV) and install MOMO's APK file on it.
- Start Wireshark again with Root access.
- Select interface to start capturing.
- Since the connection is HTTPS, the request is encrypted and the logging information does not contain sensitive information (endpoints, cookies, etc.) as in Figure 12 & 13 below.



```
▷ Frame 499: 304 bytes on wire (2432 bits), 304 bytes captured (2432 bits) on interface 0
▽ Ethernet II, Src: Apple_4f:2b:55 (28:cf:e9:4f:2b:55), Dst: 2wire_90:2d:61 (74:9d:dc:90:2d:6
  ▷ Destination: 2wire_90:2d:61 (74:9d:dc:90:2d:61)
  ▷ Source: Apple_4f:2b:55 (28:cf:e9:4f:2b:55)
    Type: IP (0x0800)
▷ Internet Protocol Version 4, Src: 192.168.1.70 (192.168.1.70), Dst: 208.82.16.68 (208.82.16
▷ Transmission Control Protocol, Src Port: 55077 (55077), Dst Port: 80 (80), Seq: 1449, Ack:
▽ Hypertext Transfer Protocol
  ▷ Data (238 bytes)
```

Figure 12. Packet Analyzer Information



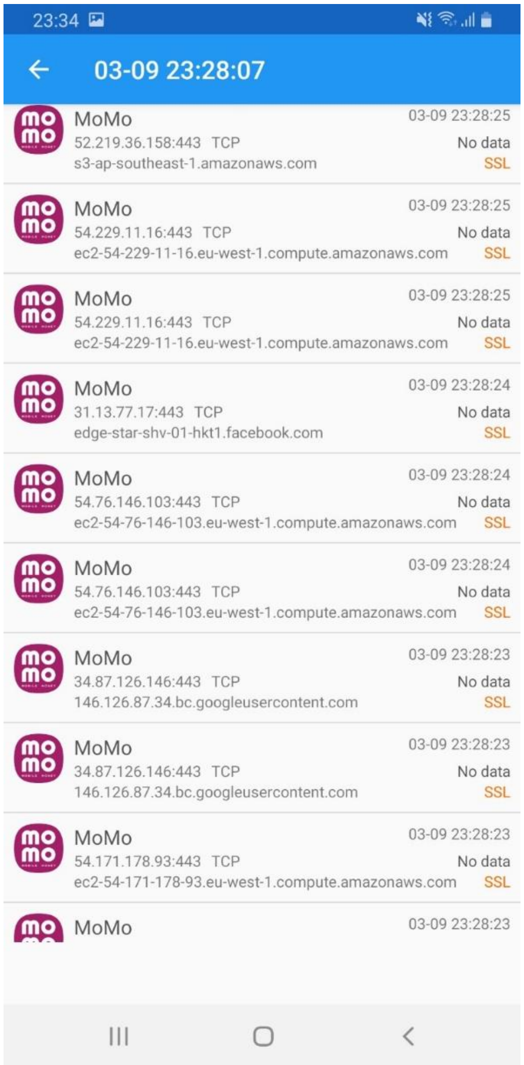
```
0000  60 36 dd a6 c5 43 10 d5  42 51 12 f3 08 00 45 00   `6...C.. BQ....E.
0010  05 1c 7b 70 00 00 71 11  71 47 55 4a 16 fd c0 a8   ..{p..q. qGUJ....
0020  2b 2a f6 e7 c1 71 05 08  73 fb 60 00 00 00 04 d8   +*...q.. s.`.....
0030  11 80 20 01 00 00 9d 38  78 cf 24 ec 09 18 aa b5   .. ....8 x.$.....
0040  e9 02 20 01 00 00 5e f5  79 fb 2c 55 3e 8e 3a 44   .. ...^. y.,U>.:D
```

Figure 13. Password encrypted (in the right corner)

When working with Packet Sniffer, the steps to be carried out are as below:

- Install Packet Sniffer software on the device (with VPN Certificate).
- Press the start button to capture packet going through.
- Choose the app you would like to monitor. In this scenario, we want to examine packets going to and from MOMO.
- Perform some activities in MOMO app, for example, logging in, checking the account balance, requesting to pay, etc.
- Then stop the capture and check for the packet that the software had inspected.
- The activities have been captured and we can see some information such as IP address, time, TCP protocol request as in Figure 14. However, we

can see that from Figure 15, all the information is encrypted and could not be viewed in plain text.



23:34

03-09 23:28:07

MoMo 03-09 23:28:25
52.219.36.158:443 TCP No data
s3-ap-southeast-1.amazonaws.com SSL

MoMo 03-09 23:28:25
54.229.11.16:443 TCP No data
ec2-54-229-11-16.eu-west-1.compute.amazonaws.com SSL

MoMo 03-09 23:28:25
54.229.11.16:443 TCP No data
ec2-54-229-11-16.eu-west-1.compute.amazonaws.com SSL

MoMo 03-09 23:28:24
31.13.77.17:443 TCP No data
edge-star-shv-01-hkt1.facebook.com SSL

MoMo 03-09 23:28:24
54.76.146.103:443 TCP No data
ec2-54-76-146-103.eu-west-1.compute.amazonaws.com SSL

MoMo 03-09 23:28:24
54.76.146.103:443 TCP No data
ec2-54-76-146-103.eu-west-1.compute.amazonaws.com SSL

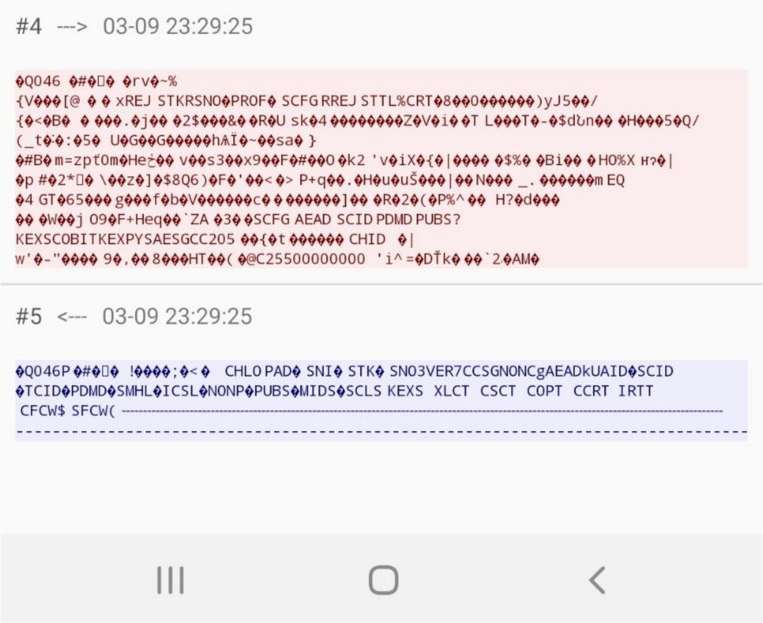
MoMo 03-09 23:28:23
34.87.126.146:443 TCP No data
146.126.87.34.bc.googleusercontent.com SSL

MoMo 03-09 23:28:23
34.87.126.146:443 TCP No data
146.126.87.34.bc.googleusercontent.com SSL

MoMo 03-09 23:28:23
54.171.178.93:443 TCP No data
ec2-54-171-178-93.eu-west-1.compute.amazonaws.com SSL

MoMo 03-09 23:28:23

Figure 14. MOMO’s Packet Capture in Packet Sniffer



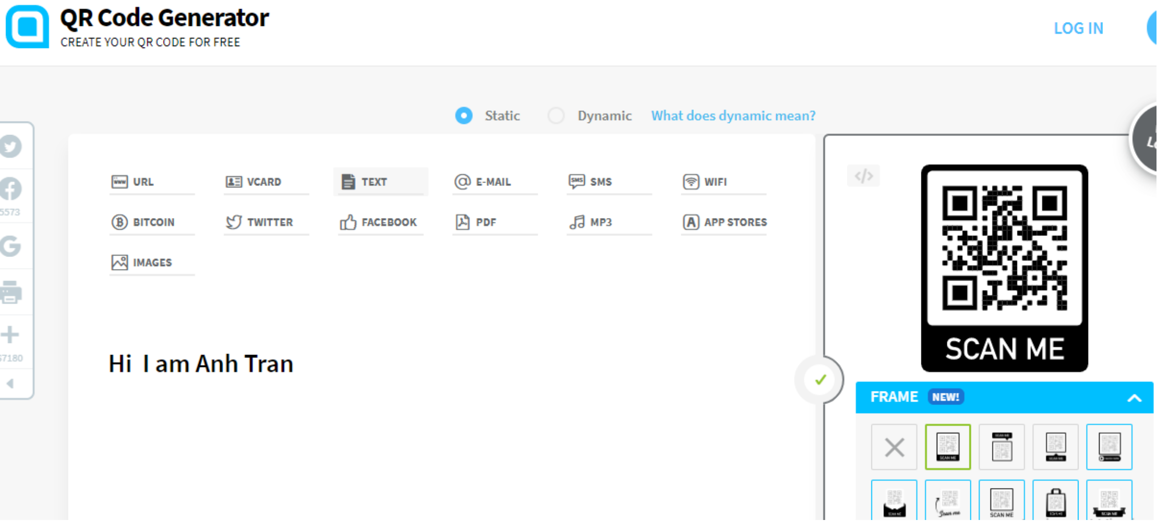
```
#4  --->  03-09 23:29:25

�Q046 �#�□� �rv�~%
{V���[@ � � xREJ STKRSNO�PROF� SCFG RREJ STTL%CRT�8��0������)yJ5��/
{�<�B� � ���.�j�� �2$���&� �R�U sk�4 ��������Z�V�i� �T L���T�-�$dǕn�� �H���5�Q/
(_t�̈�:�5� U�G��G�����hʍÏ�~��sa� }
�#B� m=zpť0m�Hẽ̲�� v��s3��x9��F�#��0 �k2 'v�iX�{�|���� �$%� �Bi�� � H0%X н?�|
�p #�2*□� \��z�]�$8Q6)�F�'��<�> P+q��.�H�u�uŠ���|�� N��� _. ������m EQ
�4 GT�65��� g���f�b�V������c� � ������]�� �R�2�(�P%^�� H?�d���
�� �W��j 09�F+Heq��`ZA �3� �SCFG AEAD SCID PDMD PUBS?
KEXSCOBITKEXPYSAESGCC205 ��{�t ������ CHID  �|
w'�-"���� 9�,�� 8���HT��( �@C25500000000 'i^ =�DŤk� ��`2�AM�

#5  <---  03-09 23:29:25

�Q046P �#�□� !����;�<�  CHLO PAD� SNI� STK� SN03VER7CCSGNONCgAEADkUAID�SCID
�TCID�PDMD�SMHL�ICSL�NONP�PUBS�MIDS�SCLS KEXS  XLCT  CSCT  COPT  CCRT IRTT
 CFCW$ SFCW( ------------------------------------------------------------------------
----------------------------------------------------------------------------------
```

Figure 15. Detail information of the Packet

It is concluded that after analyzing the packet, we could not retrieve any highly-sensitive information or any password presented in plain text. The data transmission is correctly encrypted and does not expose any vulnerabilities.

5.3 Reading a malicious QR code

The aim of this test is to check the validity of QR code (Related to the 4th threat). The test requires generating an invalid QR code from https://www.qr-code-generator.com/ to represent a text content as in Figure 16 below.

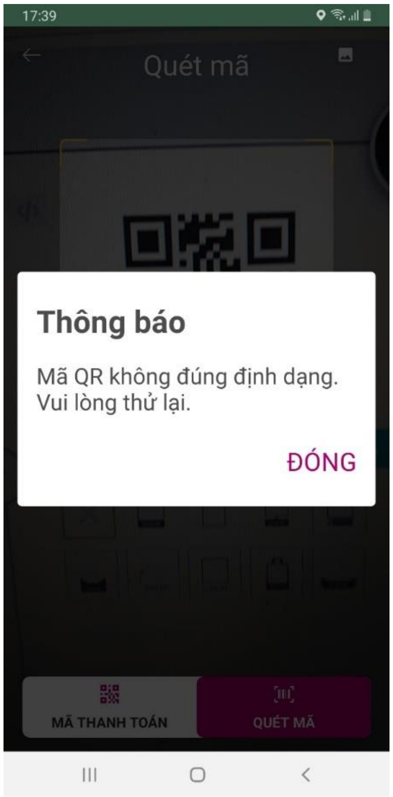


● Static ○ Dynamic

Hi I am Anh Tran

Figure 16. QR code Generator

Later, try to scan this invalid code to get response from the MOMO wallet. The result is that MOMO wallet detected this as invalid formatted. Figure 17 below shows the following: "*QR code is invalid. Please try again*.". Therefore, malicious and invalid QR code could not be used to proceed the transaction.



Thông báo

Mã QR không đúng định dạng.
Vui lòng thử lại.

Figure 17. Invalid QR code being denied

As a result, it is demonstrated that transactions cannot be processed through invalid QR codes.

5.4 Examining two-factor authentication

The aim of this test is to examine the two-factor authentication mechanism (Related to the 4th threat).

The test requires one Android Smartphone with MOMO installed to conduct logging in and perform financial transaction.

Throughout the experiment, PIN, Face ID or Fingerprint are requested every time user logs in to the phone and performs a financial activity, such as making a purchase, transfer money, etc.).

The conclusion was that the two-step authentication is implemented to increase the security level while using the application.

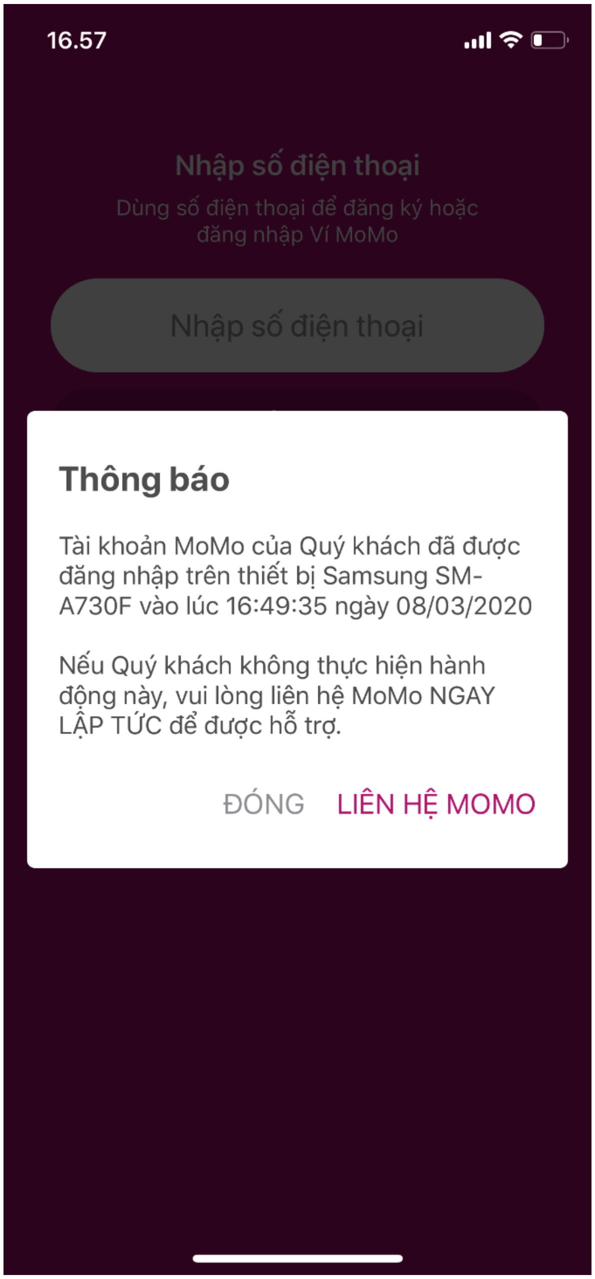
5.5 Logging in to same account in multiple devices at the same time

The aim of this test is to inspect authorization process (Related to the 4th threat).

The test requires two Android smartphones with MOMO installed.

Let’s try to login to the same MOMO account on multiple devices at the same time. Providing that the correct OTP were inserted, after successfully logged in to the second device, there will be a popup window warning about the login to a new device. We will be no longer able to access the MOMO wallet on the first device.

The figure below indicates a security warning while logging to the same MOMO account on a different device. It says: “*Your MOMO account was logged in to device SAMSUNG SM-A730F at 16:49:35 on 08/03/2020. If this activity is against your wish, please contact MOMO urgently for security support. Thank you*.”



16.57

Nhập số điện thoại

Dùng số điện thoại để đăng ký hoặc đăng nhập Ví MoMo

Nhập số điện thoại

Thông báo

Tài khoản MoMo của Quý khách đã được đăng nhập trên thiết bị Samsung SM-A730F vào lúc 16:49:35 ngày 08/03/2020

Nếu Quý khách không thực hiện hành động này, vui lòng liên hệ MoMo NGAY LẬP TỨC để được hỗ trợ.

ĐÓNG LIÊN HỆ MOMO

Figure 18. Security warning for log in to another device

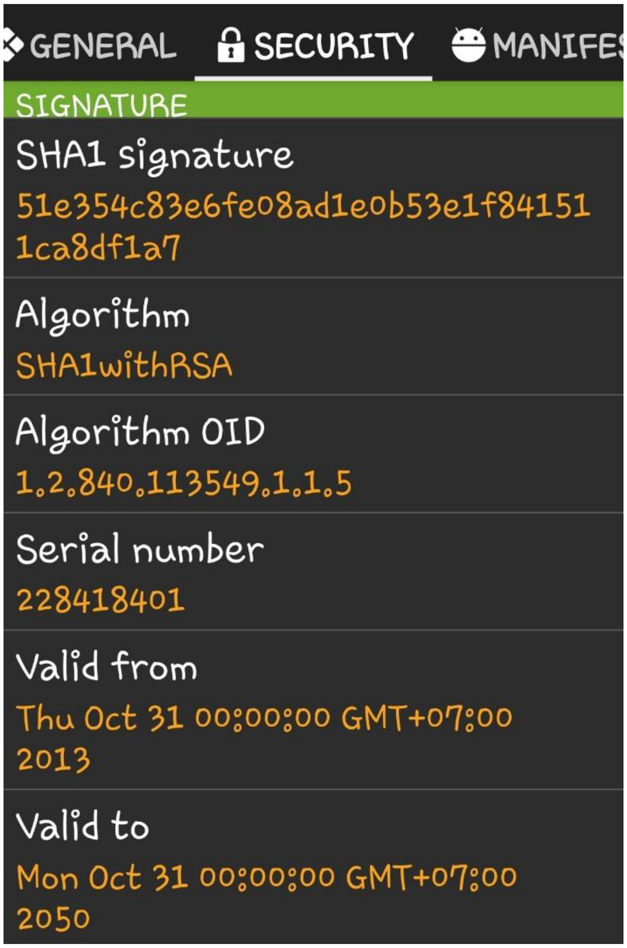
In conclusion, the system is protected against utilization of the same account on multiple devices at once.

5.6 Verifying APK Cryptography

The aim of this test is to verify the security mechanism that has been stated to be applied in MOMO application (Related to 5th threat).

The test requires an Android smartphone device with APK Analyzer installed.

Start the APK Analyzer and choose application target as MOMO. The APK Analyzer will return the security mechanism and encryption that are currently in use as in Figure 19.



SIGNATURE

SHA1 signature
51e354c83e6fe08ad1e0b53e1f84151
1ca8df1a7

Algorithm
SHA1withRSA

Algorithm OID
1.2.840.113549.1.1.5

Serial number
228418401

Valid from
Thu Oct 31 00:00:00 GMT+07:00
2013

Valid to
Mon Oct 31 00:00:00 GMT+07:00
2050

Figure 19. APK Analyzer result

The conclusion was that encryption Algorithm used is MD5, SHA with RSA signature, same as what MOMO has provided before.

5.7 Validating sensitive fields on mobile application

The aim of this test is to validate the existence of input to sensitive field on mobile application (Related to the 6th threat)

The test requires an Android Smartphone with MOMO installed and ready to log in for the first time.

For this threat, the validation of sensitive fields when logging in to MOMO is tested. Try to login from different smartphones and test with all open fields (registered phone number, password). During the next step, when connecting the digital wallet with a bank account, it is also required for correct information to proceed. All incorrect details will cause errors in the screen.

The conclusion was that in every tested flow, the fields are validated. The security mechanism is effectively implemented.

In total, seven tests were performed in order to examine MOMO's security mechanism. From the results of all the tests, it is noticed that MOMO successfully maintains security on their mobile application. Until now, no security threats are detected regarding the points mentioned above. This is a proof of high security standard in a digital wallet.

6 FUTURE TECHNOLOGY

Nowadays, the incredible improvement and innovation in security, especially in the field of mobile application, can bring in optimal solutions for mobile payment and digital wallet. The development introduces some challenges as well, which are hopefully to be solved in the meantime and contribute to the future financial payment market.

6.1 Opportunity

The rapid growth of mobile users is beneficial for mobile payment to become even more popular (2.07 billion users worldwide) (Alex 2019). Smartphones are now extended to payment systems, apart from communication and social media. It is recorded in IT Intelligence Market that four out of tens users make purchases with their phones, doubling the number of mobile payment users during the last three years (Viktoria 2019). Many attempts have been made to be ready for the replacement of traditional payment by mobile payment within the last decade. Big players in the mobile market such as Apple, Samsung, Google and PayPal did not fall behind the trend (Figure 20). They keep releasing better versions of digital wallet with superior technologies and customized interfaces. Mobile payment achieved great outcome in Europe, Asia and North America, and is expected to expand its influence across the world in other continents.

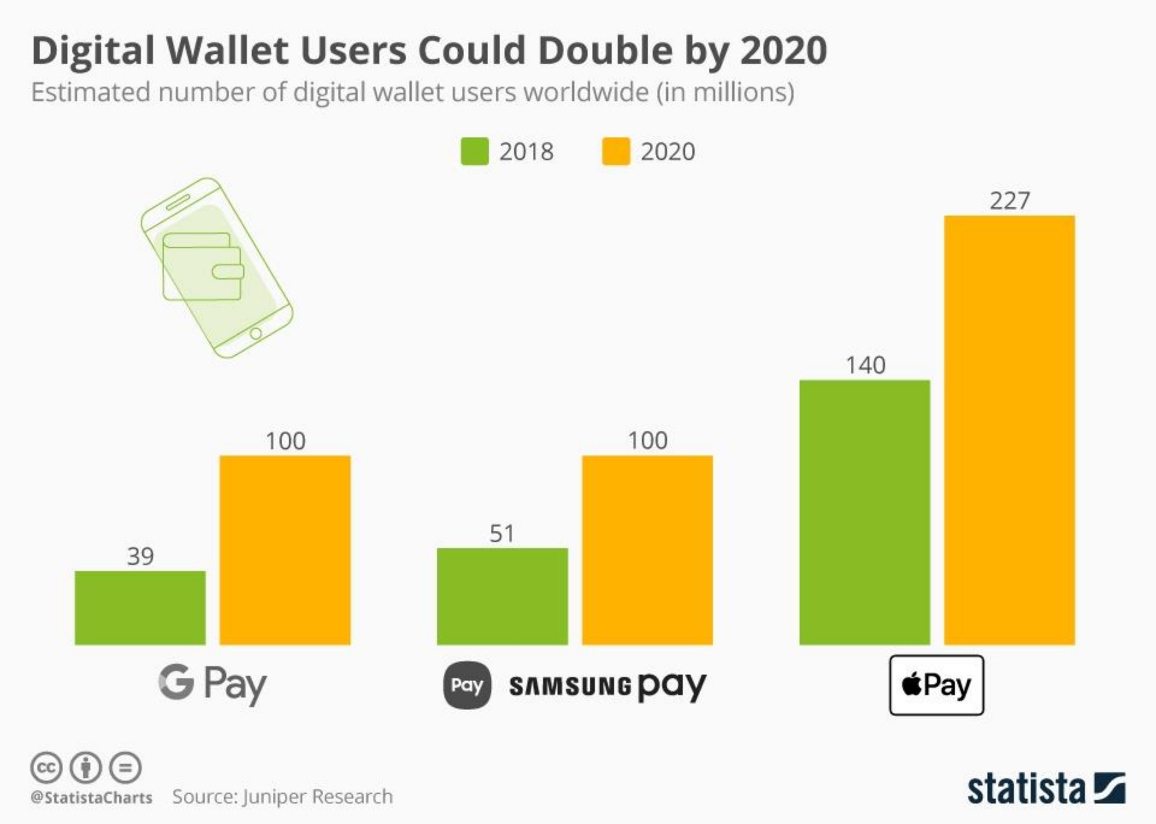


Figure 20. Digital Wallet Users estimated in 2020 (Juniper Research)

Below are a few technologies and improvements that are awaited to make enormous changes in the online commerce (Tranglo 2019):

- **Mobile payment adoption:** The adoption rate will increase by more merchants. One of the biggest limits of mobile payment is the number of merchants available for mobile payment processing. Global mobile payment transaction value is expected to reach 457 billion USD by 2026 (Global Mobile Payment Market report 2019). Demand for Mobile POS is rising.
- **Cryptocurrency:** The rise of cryptocurrency brings along the development of mobile payment: cyber currencies' popularity requires exchanging funds P2P. Mobile payment is the best solution to meet people's need.

- **Customer loyalty**: Customer engagement will be enhanced with the use of mobile payment. Service providers and retails can collect users' feedback on digital platforms and improve their customer service.
- **China becomes the leader** in cashless payment: The fastest growing market for mobile payment is China according to Bill (2018). The use of Alipay and WeChat dominated the m-commerce in China and has widespread to other countries.

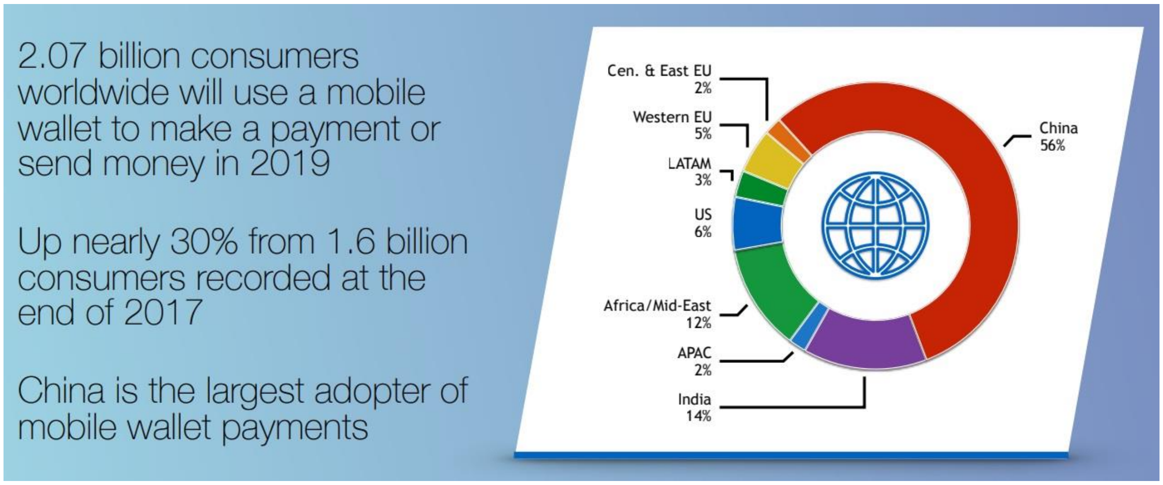


Figure 21. Worldwide Mobile Wallet (Alex 2019)

- **New techniques:** MST or Sound Wave payment are invented to extend mobile payment to people without smartphones but only normal mobiles.
- **D2P/P2P payment:** This is more common and actively involved in the online payment market.
- **Virtual Card Technology (VCT):** This is an add-on virtual visa card attached to the phone number that is prepaid and reloadable. VCT is slowly evolving and will offer a new, seamless, secure experience in mobile.
- **Biometric Authentication**: Apple plays a significant role in boosting the application of biometric authentication, from fingerprint in to face ID in 2018. It is in the hope that liable biometric authentication will reduce online fraud in payment system.
- **Dynamic cryptogram:** This cryptogram can enter the technology market and create secure payment process.

- **Remote purchase:** This purchase will dominate the global transaction business world.
- **Artificial Intelligence (AI):** Until it proves to function properly and appropriately for the payment system, we can rely on AI, a new technology that is able to prevent theft and fraud detection.
- **Virtual Reality (VR):** VR has moved beyond gaming and expanded its simulation application to retail, travel, education, movies and design. VR can make a revolution in this digitalized world.
- **Neobank**: This is a digital bank institution that enables consumers to perform banking activities via digital devices (mobile, computers, etc.) only while conventional banks do this via physical branches. Neobank is getting popular and can change the surface of traditional banking system in the near future.

With a lot of opportunities ahead, it is highly expected that mobile payment gradually becomes the primary payment option in daily life.

6.2 Challenge

Mobile payment is growing beyond consumer demand. Many elements and stakeholders are also involved in this e-commerce revolution. Together with the opportunities given, mobile payment also faces some challenges during its development (Alfred 2019).

- **Regulation and compliance**: These have always been hot topics since the dawn of mobile payment development. Governments and banking organizations must implement legal requirements for payment service providers to bind with.
- **Fraud prevention**: Customers can be reluctant to adopt mobile payment if it presents risky matters, for example leaked data, device failure and errable transactions.
- **Security issue**: This is the biggest concern of consumers when deciding on mobile payment adoption. Too many intermediates can expose

potential risks to attackers. The reputation of financial institution could be destroyed due to a loss in a bank account or identity theft. Therefore, security measures must be enhanced to prevent and detect the violations.

- **Mobile payment infrastructure:** Not all merchants are equipped with ready POS.

These challenges must be solved in order to maintain the success of mobile payment, gain the trust from customers and introduce better mobile payment service to customers.

7 CONCLUSION

The study covers theoretical study on different topics related to mobile payment service, as well as the technology commonly used to ensure the security of mobile payment in general and digital wallet in particular. The theoretical topics presented were investigated thoroughly and provide sufficient knowledge of (i) different types of mobile payment in terms of technology, advantages and disadvantages, (ii) the benefits and drawbacks of mobile payment in comparison to traditional payment, (iii) the threat model associated with all stakeholders involved in the mobile payment, (iv) security measures towards each stakeholder and (v) OWASP Top 10 of Mobile Threats as discussed in the first chapter. The theory part of this thesis explored deep understanding of mobile payment and digital wallet security threat, therefore laid a good foundation for initiating the practical part.

Thanks to the background knowledge gained from the theory part, the security testing was conducted in March 2020, focusing on MOMO’s security mechanism. The tests mostly related to the wireless communication technologies that are currently implemented in the system. In order to specify the security tests, the common threats were predefined from the security ecosystem and measures of each stakeholder (section 3.4) and classified into categories, which were referenced from OWASP Top 10 (section 4.3).

As a result, seven threats were indicated and a possible security test was performed on each individual threat. The tests allow us to discover any issues regarding MOMO security system for the digital wallet application on mobile phone. These include: Interception of NFC communication in order to gather credit card information of the consumer, Interception communication of the mobile appication, Testing against reading malicious QR code, Verify the effectiveness of two-factor authentication, Secure login to the same account in multiple devices at the same time, APK cryptography verification, and Validation of sensitive fields on mobile application. The threats identified falls into categories 3,4,5 and 6 in the OWASP Top 10. The security tests were well-prepared and conducted. However, if there are more resources and time to be spent, the cloud infrastructure and API of MOMO application can be investigated thoroughly.

After the tests, we can come to the conclusion that part of MOMO security measures are examined and still functions properly to maintain MOMO digital wallet security. The experiments were succesfully conducted and presented a good result. MOMO security system was verified against malicious threats and vulnerabilities. The security mechanism that is stated on MOMO’s website such as Two-factor authentication, Tokenization, RSA Encryption, SSL/TLS Protocol are correct and efficiently operated.

The objective of the thesis was achieved and able to determine the efficiency of the security technologies that are applied by MOMO. At the end of the study, some opportunities and challenges in the upcoming years were also introduced, giving a positive signal for mobile payment industry. The thesis can be used as a reference to contribute to later research on the constantly-developing mobile payment service.

REFERENCES

ACCEO Tender Retail Team. 2017. Cloud-based mobile payments are transforming your devices into e-wallets. WWW document. Available at: https://tender-retail.acceo.com/blog/cloud-based-mobile-payments-are-transforming-your-devices-into-e-wallets/ [Accessed 1 May 2017].

Aite Group 2016. The Evolution of Digital and Mobile Wallets. WWW document. Available at: https://www.paymentscardsandmobile.com/wp-content/uploads/2016/10/The-Evolution-of-Digital-and-Mobile-Wallets.pdf [Accessed 1 Mar 2020].

Alex R. 2019. Mobile wallet trends annual report 2019. WWW document. Available at: https://www.paymentscardsandmobile.com/mobile-wallet-trends-annual-report-2019/ [Accessed 9 Apr 2019].

Alfred 2019. The Future of Mobile Wallets: Opportunities and Challenges for the Wallet Integration**.** WWW document. Available at: https://www.dotcominfoway.com/blog/opportunities-and-challenges-for-the-wallet-integration/#gref [Accessed 14 Sep 2019].

Andrew L. 2018. Security researchers found vulnerabilities at AT&T, T-Mobile, and Sprint that could have exposed customer data. WWW document. Available at: https://www.theverge.com/2018/8/25/17781906/att-tmobile-sprint-security-vulnerabilities-customer-information [Accessed 25 Aug 2018].

Asia Tech Daily. 2019. Momo-The Rising Star of Vietnam Online Payments. WWW document. Available at: https://www.asiatechdaily.com/momo/ [Accessed 13 Feb 2019].

Bill C. 2018. Here's Why Mobile Payments Are The Future Of Commerce**.** WWW document. Available at: https://www.inc.com/bill-carmody/heres-why-mobile-payments-are-future-of-commerce7.html [Accessed 11 Jan 2018].

Bryan B. 2019. Digital Cash is Here, say Goodbye to your Wallet. WWW document. Available at: https://medium.com/mobiletopup/digital-cash-is-here-say-goodbye-to-your-wallet-ec57b2c48058 [Accessed 30 Jan 2019].

Comviva. 2016. What Are Sound Based Payments? WWW document. Available at: https://blog.comviva.com/what-are-sound-based-payments/ [Accessed 2 Jun 2016].

Corey N. 2018. Digital authentication: The past, present and uncertain future of the keys to online identity. WWW document. Available at: https://www.geekwire.com/2018/digital-authentication-human-beings-history-trust/ [Accessed 22 Sep 2018].

David Z. 2019. The Future of Payments is found in Scandinavia. WWW document. Available at: https://www.paymentsjournal.com/the-future-of-payments-is-found-in-scandinavia/ [Accessed 12 Aug 2019].

Deloitte. 2019. Chasing cashless? The Rise of Mobile Wallets in the Nordics. Available at: https://www2.deloitte.com/content/dam/Deloitte/dk/Documents/financial-services/Downloads/Chasing_Cashless-The_rise_of_Mobile_Wallets_in_the_Nordics.pdf [Accessed 10 Jan 2019].

Derrick P. 2017. WeChat phenomenon: How a messaging app helped spark China's cashless revolution. WWW document. Available at: https://www.channelnewsasia.com/news/cnainsider/wechat-china-cashless-revolution-9353998 [Accessed 29 Oct 2017].

Developers MOMO Docs. 2019. About MOMO API. WWW document. Available at: https://developers.momo.vn/#/docs/en/?id=about-momo-api [Accessed 1 Mar 2020].

Developers MOMO Docs. 2019. Security. WWW document. Available at: https://developers.momo.vn/#/docs/en/?id=security. [Accessed 1 Mar 2020].

Dierks T., Rescorla E. 2008. The Transport Layer Security (TLS) Protocol Version 1.2. Available at: https://tools.ietf.org/html/rfc5246 [Accessed 1 Mar 2020].

ECMA. 2013. Standard ECMA-352 Near Field Communication Interface and Protocol -2 (NFCIP-2). Available at: http://www.ecma-international.org/publications/standards/Ecma-352.htm [Accessed Jun 2013].

Emily S. 2018. Different types of mobile payments explained. WWW document. Available at: https://www.mobiletransaction.org/different-types-of-mobile-payments/ [Accessed 31 May 2018].

Emir E., Mehmet S. 2019. OTPaaS—One Time Password as a Service. Available at: https://ieeexplore.ieee.org/document/8439007 [Accessed 3 Mar 2019].

Emir H. 2017. Dynamic Rule Encryption for Mobile Payment. Available at: https://www.hindawi.com/journals/scn/2017/4975302/ [Accessed 26 Jan 2017].

Federal Information Processing Standards Publication 197. 2001. Announcing the ADVANCED ENCRYPTION STANDARD (AES). Available at: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf [Accessed 26 Nov 2001].

Fintechnews Vietnam. 2019. Overview of Vietnam's Major E-Wallet and Mobile Payment Players. WWW document. Available at: https://fintechnews.sg/32843/vietnam/overview-of-vietnams-major-e-wallet-and-mobile-payment-players/ [Accessed 6 Aug 2019].

Flavio M. 2015. The History of the Mobile Payment Experience #INFOGRAPHIC.

WWW document. Available at: http://winthecustomer.com/technology-changing-the-mobile-payment-customer-experience/ [Accessed 9 Jun 2015].

FT Confidential Research 2019. Red tape holds Vietnam back in digital payments. WWW document. Available at: https://asia.nikkei.com/Editor-s-Picks/FT-Confidential-Research/Red-tape-holds-Vietnam-back-in-digital-payments [Accessed 29 Mar 2019].

Gemalto. 2020. One Time Password (OTP). WWW document. Available at: https://www.gemalto.com/companyinfo/digital-security/techno/otp [Accessed 13 Feb 2020].

Guo J. 2016. MBA Thesis-The Growth & Future of Mobile Payments. Available at: https://scripties.uba.uva.nl/search?id=623960 [Accessed 1 Mar 2020].

Instituto Economía Digital ESIC. 2016. Types of Mobile Payments. WWW document. Available at: http://blogs.icemd.com/blog-moma-trends-mobile-payments/types-of-mobile-payments/ [Accessed 4 Apr 2016].

IT Intelligence Markets. WWW document. Available at: http://www.sbwire.com/press-releases/focusing-on-new-trends-for-mobile-payment-market-forecast-by-2026-with-major-prominent-key-apple-google-american-express-company-mastercard-paypal-isis-mobile-wallet-1159964.htm [Acessed 28 Feb 2019].

J.P. Morgan 2019. E-commerce Payments Trends: Vietnam. WWW document. Available at: https://www.jpmorgan.com/merchant-services/insights/reports/vietnam [Accessed 1 Mar 2020].

Jaime T. 2019. Banking & Payments for Gen Z Report: The winning strategies for attracting the next big opportunity — Generation Z. WWW document. Available at: https://www.businessinsider.com/banking-and-payments-for-gen-z?IR=T [Accessed 2 May 2019].

John R. 2016. The evolution of the mobile payment. WWW document. Available at: https://techcrunch.com/2016/06/17/the-evolution-of-the-mobile-payment/ [Accessed 17 Jun 2016].

Larke W. 2018. Norway and China in front with mobile payment. WWW document. Available at: https://scandasia.com/norway-and-china-in-front-with-mobile-payment/ [Accessed 23 Nov 2018].

Liebana-Cabanillas F., Sanchez-Fernandez J.& Munoz-Leiva F. 2015. Influence of age in the adoption of new mobile payment systems. Available at: https://www.researchgate.net/publication/287797525_Influence_of_age_in_the_adoption_of_new_mobile_payment_systems [Accessed 1 Mar 2020].

Maria V. 2019. Digital Wallet Users Could Double by 2020. WWW document. Available at: https://www.statista.com/chart/19972/digital-wallet-users-double-2020/ [Accessed 15 Nov 2019].

Matthew H. 2012. Pre-1900 utopian visions of the ‘cashless society’. Available at: https://mpra.ub.uni-muenchen.de/40780/ [Accessed 26 Sep 2019].

MOMO Vietnam. 2019. Overview and Achievements. WWW document. Available at: https://momo.vn/gioi-thieu/gioi-thieu-chung [Accessed 1 Mar 2020].

MOMO Website. 2019. FAQ-MOMO Security Mechanism. WWW document. Available at: https://momo.vn/hoi-dap/momo-su-dung-cac-cong-nghe-bao-mat-gi [Accessed 1 Mar 2020].

MyAccountGo. 2019. Pros and Cons of a Digital Wallet. WWW document. Available at: https://www.myaccountgo.com/pros-and-cons-of-a-digital-wallet/ [Accessed 1 Mar 2020].

OWASP. 2020. OWASP Top Ten. WWW Document. Available at: https://owasp.org/www-project-top-ten/ [Accessed 1 Mar 20].

Paul Z. 2001. The Day DES Died. Available at: https://www.sans.org/reading-room/whitepapers/vpns/paper/722 [Accessed 22 Jul 2001].

PCI DSS. 2011. PCI DSS Tokenization Guidelines. Available at: https://www.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf [Accessed Aug 2011].

PYMNTS. 2019. T-Mobile Data Breach Puts Personal Data Of 1M+ Customers At Risk. WWW document. Available at: https://www.pymnts.com/news/security-and-risk/2019/t-mobile-data-breach-puts-personal-data-of-1m-customers-at-risk/ [Accessed 24 Nov 2019].

Raymond Y. 2017. Mobile payment security gaps exposed at Hong Kong university. WWW document. Available at: https://www.scmp.com/news/hong-kong/law-crime/article/2113273/mobile-payment-security-gaps-exposed-hong-kong-university [Accessed 28 Sep 2017].

Ryan R. 2014. Cash Is Trash: The Future of Mobile Payment. WWW document. Available at: https://www.forbes.com/sites/techonomy/2014/01/23/cash-is-trash-the-future-of-mobile-payment/#2e8a06671596 [Accessed 23 Jan 2014].

Security Awareness. 2019. What are one-time passwords and their pros and cons? WWW document. Available at: https://resources.infosecinstitute.com/one-time-passwords-pros-and-cons/#gref [Accessed 8 Jul 2019].

The Gale Group Inc. 2014. Retina and Iris Scans. Encyclopedia of Espionage, Intelligence, and Security. [Accessed 1 Mar 2020].

Thomas L. 2013. Mobile Payment. Available at: https://rd.springer.com/chapter/10.1007%2F978-3-658-03251-7_1 [Accessed 30 Nov 2013].

Tranglo. 5 trends shaping the future of mobile payments. WWW document. Available at: https://tranglo.com/blog/5-trends-shaping-the-future-of-mobile-payments/ [Acessed 15 Nov 2019].

Tutorials Point. Cryptography Hash functions. WWW document. Available at: https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.htm [Accessed 1 Mar 2020].

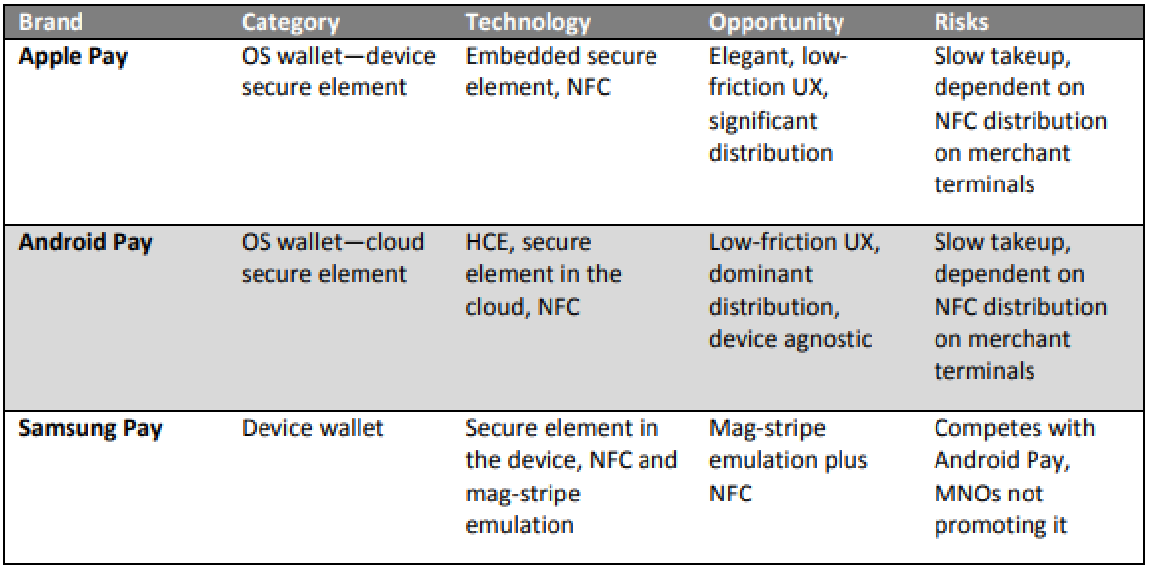
Venkatesen M. 2013. The Mobile Money Revolution. Available at: https://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000200001PDFE.pdf [Accessed 1 Mar 2020].

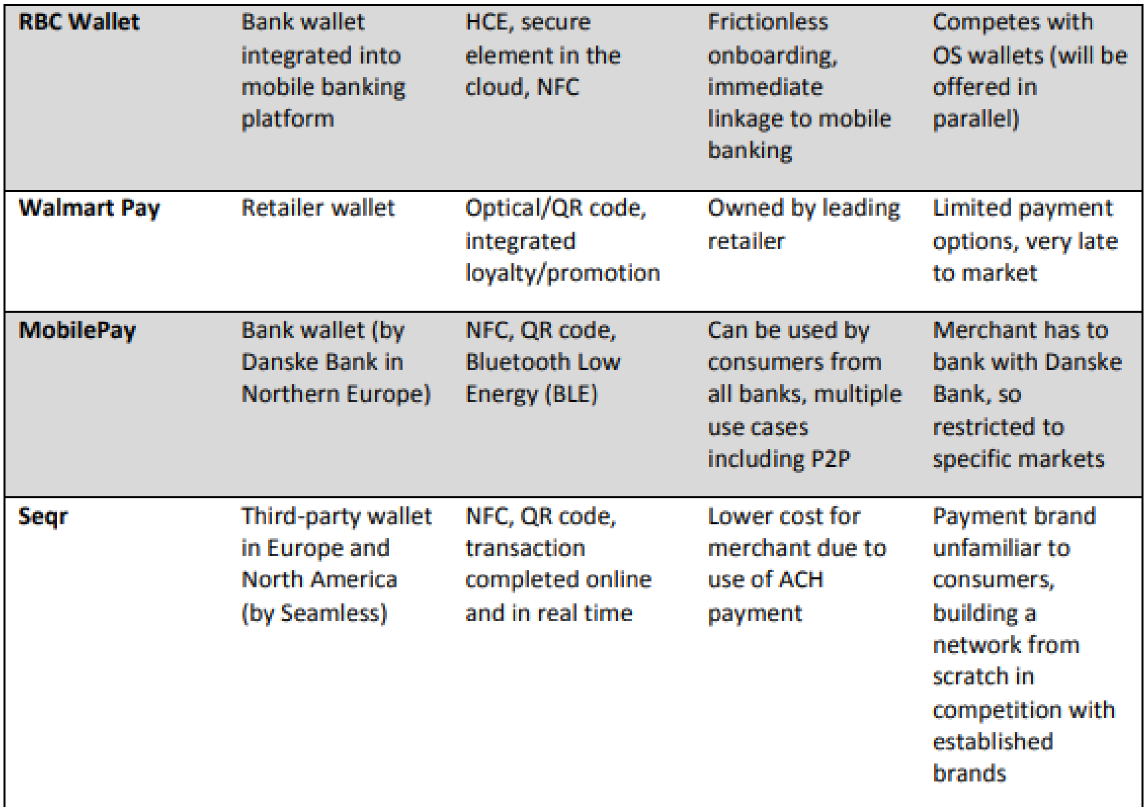
Vibha R. 2014. Overview of Mobile Payment: Technologies and Security. Available at: https://www.researchgate.net/publication/260211158_Overview_of_Mobile_Payment_Technologies_and_Security [Accessed Feb 2014].

Viktoria T. 2019. Tapping into the Future of Mobile Payments. WWW document. Available at: https://blog.globalwebindex.com/chart-of-the-week/future-mobile-payments/ [Accessed 26 Mar 2019].

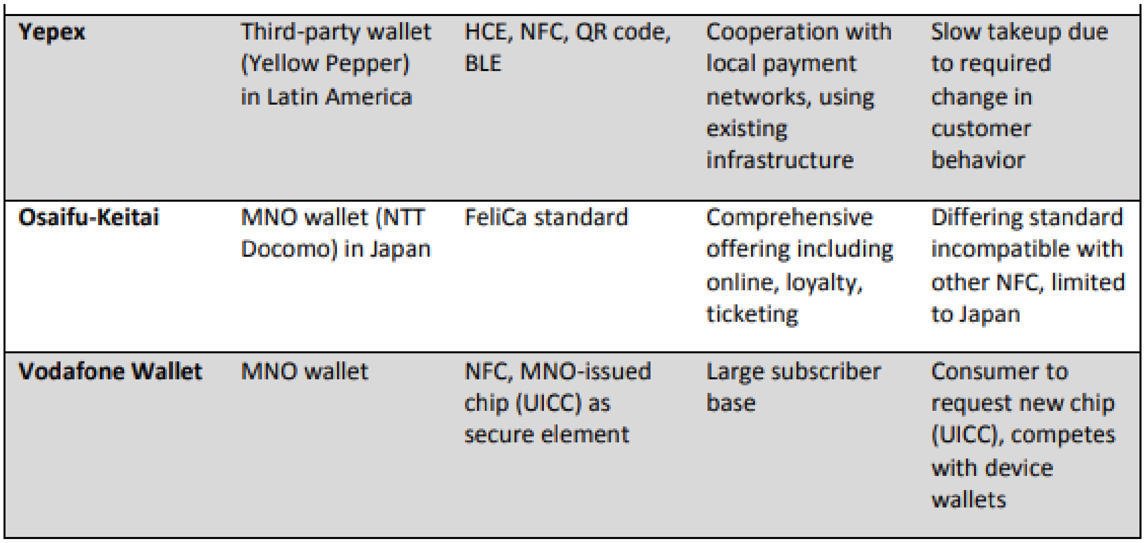
MOBILE WALLET ALTERNATIVES ANALYSIS

Below is the table that contains the comparison between the most common digital wallets to be used worldwide, regarding their category, technology, opportunity and risks. This table can be used as a useful source of reference in mobile payment.





Brand	Category	Technology	Opportunity	Risks
Apple Pay	OS wallet—device secure element	Embedded secure element, NFC	Elegant, low-friction UX, significant distribution	Slow takeup, dependent on NFC distribution on merchant terminals
Android Pay	OS wallet—cloud secure element	HCE, secure element in the cloud, NFC	Low-friction UX, dominant distribution, device agnostic	Slow takeup, dependent on NFC distribution on merchant terminals
Samsung Pay	Device wallet	Secure element in the device, NFC and mag-stripe emulation	Mag-stripe emulation plus NFC	Competes with Android Pay, MNOs not promoting it
RBC Wallet	Bank wallet integrated into mobile banking platform	HCE, secure element in the cloud, NFC	Frictionless onboarding, immediate linkage to mobile banking	Competes with OS wallets (will be offered in parallel)
Walmart Pay	Retailer wallet	Optical/QR code, integrated loyalty/promotion	Owned by leading retailer	Limited payment options, very late to market
MobilePay	Bank wallet (by Danske Bank in Northern Europe)	NFC, QR code, Bluetooth Low Energy (BLE)	Can be used by consumers from all banks, multiple use cases including P2P	Merchant has to bank with Danske Bank, so restricted to specific markets
Seqr	Third-party wallet in Europe and North America (by Seamless)	NFC, QR code, transaction completed online and in real time	Lower cost for merchant due to use of ACH payment	Payment brand unfamiliar to consumers, building a network from scratch in competition with established brands



Yepex	Third-party wallet (Yellow Pepper) in Latin America	HCE, NFC, QR code, BLE	Cooperation with local payment networks, using existing infrastructure	Slow takeup due to required change in customer behavior
Osaifu-Keitai	MNO wallet (NTT Docomo) in Japan	FeliCa standard	Comprehensive offering including online, loyalty, ticketing	Differing standard incompatible with other NFC, limited to Japan
Vodafone Wallet	MNO wallet	NFC, MNO-issued chip (UICC) as secure element	Large subscriber base	Consumer to request new chip (UICC), competes with device wallets

Figure 22. Mobile Wallet Alternatives (Aite Group)