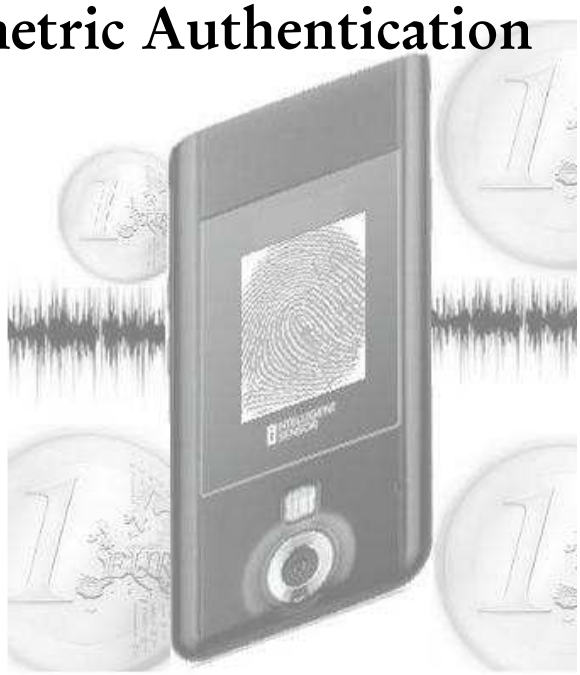
Master Thesis

Information Management
Faculty of Computer Sciences
University of Koblenz-Landau

Biometric Authentication



in Mobile Payments

Supervisors:
Prof. Dr. J. Felix Hampe
Stefan Stein

Submitted by:
Shiny Sreekumar
201 210 414
Gudenauer Weg 57
53127 Bonn
shiny@uni-koblenz.de

Koblenz, September 2010

Acknowledgements

I would like to acknowledge and thank all the people who contributed, in different ways, to the completion of this thesis:

- Professor Dr. J. Felix Hampe for his guidance and support always and for pointing me in the right direction with new ideas. Above all, I am thankful for his undying patience.
- Stefan Stein for his friendly assistance at all times.
- Professor Elaine Lawrence and Dr. Agnieska Zmijewska who, through email exchanges, sent me relevant papers and answered any queries I might have had.
- Lee Barr for the numerous iterations of proof-reading and pep-talks.
- My mother and my dear friends for all their help, patience and understanding.

Most of all, I would like to thank Alexandra Bohnet for constantly pushing, believing and the final "This is it" weekend! Without her, I could not have done this.

Shiny Sreekumar
Bonn, September 2010.

Picture on title page put together by author using following sources:
Pantech PG6200 Phone - (PC Welt, 2006); Fingerprint – (O'Gorman, 1999)
Sound wave – *www.nanobioart.com/nanolab/category/day7*; Euro – *www.wikipedia.org/wiki/Euro*

Abstract

Mobile payment has been a payment option in the market for a long time now and was predicted to become a widely used payment method. However, over the years, the market penetration rate of mPayments has been relatively low, despite it having all characteristics required of a convenient payment method. The primary reason for this has been cited as a lack of customer acceptance mainly caused due to the lack of perceived security by the end-user. Although biometric authentication is not a new technology, it is experiencing a revival in the light of the present day terror threats and increased security requirements in various industries. The application of biometric authentication in mPayments is analysed here and a suitable biometric authentication method for use with mPayments is recommended. The issue of enrolment, human and technical factors to be considered are discussed and the STOF business model is applied to a BiMoP (biometric mPayment) application.

Keywords: Biometric Authentication, mPayments, Speaker Recognition, Fingerprint Recognition, Enrolment, Customer Acceptance, STOF Model.

Table of Contents

List of Figures

List of Abbreviations

AFIS	Automated Fingerprint Identification System
ATM	Automatic Teller Machine
ATV	Ability-to-Verify Rate
BiMOP	Biometric mPayment
C2C	Customer-to-Customer
CDI	Critical Design Issue
CDMA	Code Division Multiple Access
CRM	Customer Relationship Management
CSF	Critical Success Factor
ECBS	European Committee for Banking Standards
eCommerce	Electronic Commerce
EDY	Euro Dollar Yen
EER	Equal Error Rate
ePayment	Electronic Payment
EU	European Union
FAR	False Acceptance Rate
FMR	False Match Rate
FNMR	False Non-Match Rate
FRR	False Rejection Rate
FTE	Failure-to-Enrol Rate
GSM	Global System for Mobile Communications
GSMA	GSM Association
HSB	Hanauer Strassenbahn AG
ICICI	Industrial Credit and Investment Corporation of India
ID	Identification
IRCTC	Indian Railway Catering and Tourism Cooperation
ITU	International Telecommunication Union
IVR	Interactive Voice Response
JCB	Japan Credit Bureau
mCommerce	Mobile Commerce
MMS	Multimedia Messaging Service
MNO	Mobile Network Operator

MP	mPayment
MPRM	Mobile Payment Reference Model
mPayment	Mobile Payment
MPSP	Mobile Payment Service Provider
MSISDN	Mobile Subscriber Integrated Services Digital Network
mTicketing	Mobile Ticketing
MVNO	Mobile Virtual Network Operator
NAB	National Australian Bank
NFC	Near-Field Communication
P2P	Peer-to-peer
PDA	Personal Digital Assistant
PIN	Personal Identification Number
PNR	Passenger Name Record
PoC	Price of Convenience
POS	Point-of-Sale
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RBC	Royal Bank of Canada
RCMP	Royal Canadian Mounted Police
RFID	Radio Frequency Identification
RMV	Rhein-Main-Verkehrsverbund
ROI	Return on Investment
SIM	Subscriber Identity Module
SMS	Short Messaging Service
STOF	Service, Technology, Organization and Finance
Telco	Telecommunication Provider
UAE	United Arab Emirates
UK	United Kingdom
UOB	United Overseas Bank
USA	United States of America

1. Introduction and Overview

This thesis will deal with the issue of authentication in mPayments and how this could be realized using biometrics with the goal of developing a viable business model. A special focus is given to the process of enrolment as it forms the basis for an accurate authentication process, as well as to customer acceptance: without which the application will not be successful.

The way mankind pays for goods or services has come a long way from the early barter system. There now is a plethora of payment options available ranging from cash to plastic cards to electronic payment (ePayment) techniques, from which the consumer can choose the payment method most convenient to him. One of the payment options available today – although not widespread – is mobile payments (mPayment). In its simplest form, mPayment can be defined as "*payments that are carried out via the mobile phone*" (Krueger, 2001, p. 1).

Although it was predicted that mPayments would be very successful and would be the chosen form of payment for many customers (Krueger, 2001), there are only a limited number of mPayment applications in the market and these have not been able to achieve the expected level of market penetration. In his paper on the problems of mPayment in Europe, Pousttchi states two reasons for this: the lack of necessity for a new payment method and the user's perception of the low levels of security in mPayments (Pousttchi, 2004). Based on the study of a failed Swiss mPayment application, (Ondrus et al., 2009) found that the mPayment application failed to offer real value to the consumers as well as lacked a non-standard solution, amongst others.

To be an attractive payment option to the user, mPayment has to offer some value over the existing payment methods available. In comparison to other payment options, mPayment does have its advantages, the prime one being a higher level of convenience. MPayment could minimize, if not eliminate, the need to carry around plastic cards and cash; the only object the user would have to carry on him would be his mobile device. With this added advantage of convenience over other

payment options, the other prime hindrance that mPayment needs to overcome is the user's perception of mPayment security.

Security in payment applications is established by means of successful user authentication. Authentication can be defined as *"the ability to confirm"* a claimed identity (Creese et al., 2003, p. 2). The most common form of authentication in payment systems is carried out by means of knowledge-based techniques like Personal Identification Numbers (PINs). Authentication can also be carried out using object-based authentication and biometric-based authentication. These different types of authentication methods are further explained in Chapter 3.

Since authentication essentially opens the access gateway to whatever object it secures, it could be said that the level of security of any application depends on how robust the authentication process is. If the user considers the authentication process to be foolproof, he would potentially perceive the application to be secure. This leads to the question of which authentication method and process would be best-suited for use in mPayment applications in order to gain the trust of the user. Would the traditional PIN/password authentication method suffice or would a more sophisticated, "newer" method be required?

Enter Biometrics. Biometrics can be defined as *"the automated use of physiological or behavioural characteristics to determine or verify identity"* (Nanavati et al., 2002, p. 9). Biometric authentication is used in various sectors like law enforcement, healthcare, the government sector, travel & immigration as well as the financial sector (Nanavati et al., 2002). Major European airports like Amsterdam Schiphol, Fraport Frankfurt, various UK airports as well as airports in Canada and the United Arab Emirates (UAE) use iris recognition for automated border controls (Bohnet, 2009). Many European Union (EU) passports employ face recognition with machine readable passports (or ePassports). The United States of America (USA) use fingerprint verification to verify travellers to their country as well as using face recognition in e-Passports (US Bureau of Consular Affairs, 2009). Biometrics are also used in more commercial contexts like simply securing a laptop with fingerprint verification.

As is illustrated in the above paragraph, biometrics are used in many diverse fields and is not, by itself, a new technology. This widespread use of biometrics ranging from the simple securing of laptops to homeland security shows that if the right biometric is chosen, it can be employed to secure any type of goods/services; hence the thought to identify if biometric authentication could be used in mPayment applications and if so, which biometric would be most appropriate.

1.1. Motivation

Payment plays an important role in everyday life. Be it a buyer going to a regular brick-and-mortar store, a buyer of digital goods, a traveller, a consumer at a vending machine or a payer of bills – they all need to pay for their goods. Typically, these payments are made through cash, credit or debit cards, which the consumer carries on him at almost all times. mPayments have been around long enough to have grown into an everyday payment option. Theoretically, it fulfils all requirements that are expected of a payment system. Soaring penetration rates of mobile devices in the market and the fact that a person owning a mobile device carries it with him almost all the time should render it a more convenient option to pay with. However, it is still far from being a common payment type. Lack of customer acceptance based on the perceived security, the costs involved and the lack of necessity for a new payment option are quoted as causes for this (Pousttchi, 2004).

Similarly, biometric security has also been around for a long time and is technically not a new invention. However, with the current global security threats, new importance is being given to biometric technologies that may offer better protection against fraud.

Although a lot of research has been done on mPayments and biometrics separately, there are only very few academic or even commercial references that combine the two. The possibility of providing reliable security in mPayment by means of biometrics, and thereby reducing the acceptance inhibition of the present day consumer, is what motivated the author to follow this line of investigation.

1.2. Scope of the Thesis

There are a number of issues that need to be resolved for mPayments to become a successful mode of payment. These include standardization of the mPayment procedures, alliances and partnerships between the players, customer acceptance and security (ECBS, 2003; Hampe et al., 2003a; Henkel, 2001a), amongst others. For the scope of this thesis, the issues concerning security and customer acceptance have been analyzed and discussed and a business model is proposed.

Security is an umbrella term that encompasses authentication, encryption, data integrity, non-repudiation and confidentiality (Hampe et al., 2003a). This thesis will concentrate on the authentication aspect of security as implemented in an mPayment system. It considers the present authentication techniques and explains how biometric authentication can be used as a counterpart to the existing methods. In the context of biometrics, this thesis narrows down to the methods of speaker verification and fingerprint reading as appropriate authentication methods in mPayments. A criteria catalogue is developed and used in Chapter 3 for this purpose. Enrolment plays a major role in successful biometric authentication and is also highlighted within this thesis. The hypothesis of amalgamating mPayments and biometric authentication and the factors that need to be considered for its implementation is the focus of this thesis.

1.3. Research Questions

This thesis aims at answering the following questions by the end:

1. ***How is customer authentication done in contemporary mPayment applications?***
2. ***Is biometric authentication more suitable than contemporary authentication methods?***
3. ***If yes, what factors should be considered during the biometric enrolment process?***
4. ***Which biometric is best-suited for use in mPayment? Why?***

1.4. Research Methodology

This work being a working hypothesis, there are only few references that directly address the issue under focus. The research work for this thesis was of exploratory nature. Academic resources and conference proceedings form a large part of the literature review for mPayment, it being a rather young research domain. Seminal literature in the field of biometrics was used and was supported by conference proceedings and journal articles. Surveys, forecasts, professional websites, patents, news reports, press releases were also referred to in order to get a picture of the present market.

1.5. Thesis Structure

The thesis will cover the topics of mPayment and biometrics and how these can be combined to provide a secure payment system. Following Chapter 1 which provides the motivation and scope of the thesis, lists the research questions and research methodology, a brief introduction on mPayments is given in Chapter 2. This chapter will also discuss the Mobile Payment Reference Model (MPRM) as given by (Pousttchi, 2005) as well as the mPayment value chain. The chapter concludes with a description of existing security measures in mPayments. Chapter 3 deals with the basics of biometrics and why biometric authentication is suited for mPayment systems. Also, a criteria catalogue is derived which is then used to identify which biometric is most suitable for mPayment applications. An introduction to speaker verification and fingerprint verification is given in this chapter. Current implementations in the field of mPayments and biometrics globally are discussed in Chapter 4. Having had a look at the mPayment and the biometric overview, Chapter 5 discusses the chief issues to be considered in using biometrics with mPayments, specifically for fingerprint verification and speaker verification. The crucial issue of enrolment alongside customer acceptance issues round up this chapter. Chapter 6 looks at scenarios of *"biometric mPayment" (BiMoP)* applications and presents a potential business model, based on STOF (Service, Technology, Organization and Finance). The final chapter of the thesis contains the summary and the conclusion & future outlook where the entire concept of biometric mPayment is assessed along with its feasibility in the market today and in the future.

2. Mobile Payments – An Overview

According to early research, mPayments were supposed to become a payment norm in the retail world (Krueger, 2001). Affordable, multi-functional mobile devices were considered to be the perfect instruments to hold a payment utility, making it more convenient to the user as plastic cards would become redundant. Although mobile devices were and still are affordable, multi-functional and have become a necessity, mPayments have not been as successful or popular as predicted. This is because the consumer does not seem to require a new payment method and is perfectly satisfied with the existing choice – cash, debit cards, credit cards, and in some countries such as the UK and the United States, even cheques. With these payment options that the consumer is accustomed to, a new payment option would not seem attractive unless it provides a certain degree of added value over the other existing payment options. The main benefit that mPayment holds over other payment options is convenience. Given that everybody who owns a mobile device carries it on him almost always, the need to carry cash is minimized and plastic cards could be completely eliminated when using mPayments. Also, if sufficient merchants accept mPayments, it holds the potential to become an ubiquitous payment option that the consumer can use anytime, anywhere. According to (Karnouskos, 2004), mPayments still hold the potential to become a standardised payment method, provided the consumer recognizes its benefits. Added to this, the companies/players providing the service should see a benefit in offering the service as well; this could be a financial profit, enhancing customer experience to promote the relationship with the customer, or revenue through some other source that's tied together with the new payment option.

2.1. Definition

In its simplest form, mPayments are defined as "*payments that are carried out via the mobile phone*" (Krueger, 2001, p. 1). This basic idea is reflected by many authors like (Ondrus et al., 2004, p. 4; Stroborn et al., 2004, p. 75). (Karnouskos, 2004, p. 44) extends this definition by including the tasks that the mobile device

performs in an mPayment transaction or rather what the mobile device has to do so that a payment transaction is classified as an mPayment transaction. *"Any payment where a mobile device is used in order to initiate, activate and/or confirm this payment can be considered a mobile payment"*. Henkel looks at mPayment from the perspective of authorizing the transaction and says *"Mobile payment refers to payment systems that use the mobile phone in the payment process, in particular for payment authorization"* (Henkel et al., 2002, p. 1).

Stroborn's definition in (Stroborn et al., 2004, p. 75) takes a slight technical inclination and states that *"Mobile payment includes all procedures that, even in the broadest sense, require the system-based usage of a mobile device for carrying out a payment process."* According to this definition, mPayment would be the set of all payment procedures that make even the slightest use of a mobile device to carry out the payment transaction.

A detailed definition is given by (ECBS, 2003, p. 6) wherein mPayment is *"not by itself a new payment instrument but an access method to activate an existing means of payment for financial transactions processed by banks between bank customers. An m-payment involves a wireless device that is used and trusted by the customer. M-payments may be card-based or non-card-based, in both the real and virtual world."* This definition only covers a bank-centric mPayment system meaning that only those transactions that involve a bank, its customers and a wireless device would fall under the category of mPayment. This would declassify payments made for purchases like the download of mobile games, logos and ring tones as mPayment transactions since these do not necessarily involve a bank. If the customer uses a prepaid mobile account, the charge is directly deducted from his stored value for which the involvement of a bank is not required. In this context, (Mallat et al., 2003) relates a problem to the simple definition of mPayments; as per the simple definition, the purchase of logos and ringtones for the mobile device would be considered as mPayment scenarios. If this were so, then one can reason that a large part of mobile phone users, if not all, have tried mPayments at least once.

Of interest from the definition of (ECBS, 2003) is the fact that it mentions the environment in which mPayment can be used. It specifies that mPayment can be used in both the *"real world"* referring to a Point-of-Sales (POS) transaction as well as in the *"virtual world"* referring to eCommerce and mCommerce. This idea of being able to use your mobile device in all possible purchasing scenarios is a strong argument that speaks for mPayment in terms of consumer convenience.

In his dissertation, Pousttchi differentiates the payment framework into mobile billing and mobile payment. He defines mobile billing as the charging/billing of telecommunication services through a mobile network operator in the context of an existing billing relationship. He further proceeds to define mPayment as *"the type of payment transaction settlement in which at least the payer uses mobile communication techniques (in connection with mobile devices) for the initiation, authorization or realization of the payment in the context of an electronic procedure"* (Pousttchi, 2005, p. 21). This kind of a differentiation between mobile billing and mPayment could be used to classify ringtone purchases more as mobile billing transactions than mPayment transactions.

From the above collection of definitions, it is obvious that while the basic idea behind mPayment is the same, the definitions only vary in their perception. While (Stroborn et al., 2004) give a more technical definition, (ECBS, 2003) defines mPayment from a bank's perspective. What remains common is the core notion behind mPayment: it is not possible without a mobile device.

Consolidating the focal aspects of the above explanations:

> *"MPayment can be defined as a payment transaction carried out with the help of a mobile device in an mCommerce, eCommerce or POS environment, wherein the mobile device is used to either initiate, activate, confirm, authorize and/or realize the payment process or transaction. The mobile device can also simply be the storage unit that warehouses the significant payment details*".

2.2. Important Aspects of mPayments

To establish the framework and area covered by this thesis, a few essential characteristics of mPayment will be described in this section. Till date, there have been numerous attempts at introducing a successful mPayment application around the world. While many have had to cease operations like Paybox (Ding et al., 2003) and Simpay (Finextra, 2005) for instance, a few mPayment systems have crystallized out successfully. The most successful and sustainable employment of mPayment has been in mobile ticketing in different transportation facilities and the purchase of parking tickets. mPark is a facility that offers paying for parking using mPayments and is available in the UK, Germany, Ireland and Australia[1]. *Deutsche Bahn* in Germany offers mobile ticketing facilities; which is explained in Chapter 4.

2.2.1. Classification of mPayment Transactions

mPayment can be used in different environments, independent of the physical location of the user and the mobile device. With reference to the environment, mPayment transactions can be classified as follows (Hampe et al., 2003b):

(a) Local transaction: A local transaction is where the mobile device is present at the payment terminal like a store POS or an Automatic Teller Machine (ATM) and it communicates locally with the payment terminal (Karnouskos, 2004). Local transactions are also known as proximity payments or contactless payments because the payment takes place in close proximity to the terminal via short range wireless communication technology (Hampe et al., 2003b) like Bluetooth, Near Field Communication (NFC) or infrared. An example of a local transaction is paying for a drink from a vending machine as offered by the MNO, Telstra in Australia known as "*Dial-a-Coke*". Using this, customers dial the number given on the vending machine and follow the given instructions to select and pay for the chosen drink; the customer is then charged for the amount in his next bill[2].

[1] www.mpark.com
[2] http://www.ccamatil.com/files/1/FINAL%20Coke%20Perth%20release.pdf

(b) Remote Transaction: A remote transaction is a payment transaction that takes place irrespective of the consumer's location (Karnouskos, 2004). When buying a bus ticket, logos, ringtones or games (digital goods), the consumer could be anywhere. These are examples of remote environments where the location of the consumer while initiating the payment is insignificant. Such payments can be browser-based as in the case of digital goods or SMS-based as in the case of mTicketing (Hampe et al., 2003b).

(c) Transactions in a personal environment: A transaction in a personal environment is a payment that takes place between several devices that are controlled by the user (Hampe et al., 2003b). An example of this could be topping up the credit on a prepaid mobile account from another mobile device using mPayment. A parent could transfer airtime to the mobile device of a child, for instance. NGPay, one of the mPayment applications in India, plans on offering such intra-mobile money transfer through their application. NGPay is also further discussed in Chapter 4.

The reason these transaction environments are listed is because the biometric mPayment application as described in this thesis is an ubiquitous one that can be used in any of these environments. What each of these transactions have in common is the payment life cycle.

2.2.2. Players in the mPayment Scenario

Players are the different entities involved in an mPayment scenario who contribute to the mPayment set-up in one way or the other depending on their core competency. These entities can be organizations, companies or individual persons. The players directly involved in the mPayment process are referred to as active players. These are the players that directly influence or are a part of the payment life-cycle depicted in Figure 1. Banks and Mobile Network Operators (MNO) are examples of active players. Passive players are players who do not directly contribute to the mPayment life-cycle, but who have a supportive role in the provision of mPayments.

Active Players

Mobile Network Operators: MNOs are the telecommunication providers (Telco) who are responsible for the network infrastructure. Their core business is running a mobile network (Pousttchi, 2004) and billing their customers for used air-time. In practice, there are two kinds of telcos – the MNOs and the mobile virtual network operators (MVNO). While MNOs have their own infrastructure, MVNOs rely on/use the network infrastructure of an MNO to provide their services. Their contribution to the value chain is the partial provision of MNO services (Pousttchi, 2005). An example of an MVNO in Germany is easymobile[3], which uses the network of the MNO, T-Mobile.

An MNO could be regarded as an ideal candidate to offer mPayment. For MNOs, billing for mPayment transactions would only involve minimal costs, if any at all, (Pousttchi, 2005) since there already exists a billing relationship with the customer . Secondly, they own and control the technical infrastructure and already provide mobile phone services. Given the huge customer database that they have (Karnouskos, 2004), MNOs could reach out to potential mPayment consumers and target their marketing efforts directly at them based on existing consumer behaviour. For instance, consumers who are early adopters of technology might be more prone to try mPayments or at least be interested in what mPayments are.

MNOs can take up to three different roles in an mPayment scenario. They can be the mobile payment service provider (MPSP) offering the mPayment service. The MNO can also take over the role of being only the billing entity. In many mPayment applications in the micro-payment sector, it is the MNO who ultimately bills the customer for his purchases using mPayment; they would function like banks that offer credit cards in card payment applications. The best example is once again the download of logos, ringtones and games. The customer buys goods and is billed by the MNO with his regular bill. The position from which the MNO has the least involvement is as a pure carrier. In such a case, the MNO is merely responsible for the transfer of payment data between the various

[3] www.easymobile.de

other players. Whatever the degree of involvement, mPayment cannot take place without the MNO in the value chain.

Banks: Banks and other financial providers like credit card companies constitute the other large player in the mPayment scenario. What makes banks attractive as the mPayment provider is the customer trust that they enjoy (Krueger, 2001). Banks have long existed in business and the customer is used to entrusting his money with the bank. Introducing an mPayment application under the banner of a bank boosts customer acceptance since the trust the customer has in the bank is transferred to the payment application. Also, their core competency being monetary transactions, banks have the required experience and risk management facilities to handle mPayment transactions (Zmijewska et al., 2006) not to mention that they have an existing payment infrastructure and vast merchant database. As an acquirer, banks have an existing number of merchants who partner with them for debit and credit card payments. This gives banks a good starting point if the merchants cooperate and agree to offer the given mPayment application as a payment option.

In a bank-dominated model, the bank is the prime player in the value chain. In such a case the bank is the player offering the mPayment application, relying on the MNO as the data carrier. Although banks do not "bill" customers, they can still be responsible for accepting the payment on behalf of the mPayment provider by simply deducting it from the customer's bank account (if the customer has an account in the given bank) or by initiating the transfer of money from the customer's account in another bank. As in the case of MNOs, the degree of involvement can vary for banks too. They can take on the role of the mPayment provider; they could be responsible only for the payment infrastructure or they could be merely handling the clearing and settlement of funds.

***Merchants*:** The role of merchants in the successful functioning of an mPayment system is often underestimated. Merchants are as important as the end-user is in the mPayment scenario. For a consumer to adopt mPayment, a substantial number of merchants need to offer it as a payment option. The greater the number of users for a given payment system, the more worthwhile it is for the merchant to

implement the payment system, and conversely, the greater the number of merchants, the more worthwhile it is for the customer to start using the payment system (Henkel, 2001a). This unfortunately forms a vicious circle; the consumer may hesitate trying out a new payment system if he cannot use it widely. The merchant, on the other hand, may not be willing to offer a new payment system if he is not convinced of a strong consumer acceptance.

It could be argued that merchants are more passive than active players. However, the author finds that since merchants strongly influence the success of mPayments and since they are directly involved with the payment system, they can be classified as active players.

Third Party Players: A third party player is an independent mPayment service provider who is neither a bank nor an MNO, but who provides an mPayment solution. NGPay for instance, which is further explained in Chapter 4, is an example of a third party driven mPayment solution. Third party players are usually start-ups and they depend on MNOs, either in a partnership or just as a carrier. The involvement of an established player like a bank or MNO helps the third party player to market its mPayment application better – an aspect required to gain the trust of its customers and to obtain a large number of both customers and merchants to use the new mPayment solution.

Passive Players

***Mobile Device Manufacturers*:** As a passive player, the mobile device manufacturer only indirectly influences the mPayment system. In present day mPayment scenarios, the mobile device manufacturers do not have a big role to play. Equipping mobile devices with adequate software and hardware required for mPayment could possibly be the responsibility of the mobile device manufacturer. This software could include mWallets, payment enabling applets, etc. However, most software that would be required can also be made available to the users as downloads from the internet and there is no additional hardware requirement for the present day mPayment applications. If however, the mPayment application is to use biometric authentication, then additional hardware such as the fingerprint reader are required.

In terms of its role in the mPayment value chain, the device manufacturer is primarily responsible for the hardware components required for mPayment. The role of the mobile device manufacturer can be illustrated using proximity payment as an example. The NFC interface/unit over which the payment data are transmitted needs to be implemented in the device. An example of such a contactless mPayment solution is the mTicketing facility in the city of Hanau, Germany which is explained in detail in Chapter 4.

Since the NFC functionality or other hardware equipment in the mobile device is not solely present for mPayment purposes, the device manufacturer would not necessarily fit into the mPayment value chain; although it is true that the equipment is not used solely for mPayment, they still form a vital element that the payment process cannot do without and hence places the device manufacturer in the position of a passive player.

Equipping the device with an mWallet is an example of how the device manufacturer might contribute to the mPayment value chain. These mWallets are usually password-protected. This provides a good level of security since essentially two levels of authentication have to be gone through, the first being entering the PIN for the SIM (Subscriber Identity Module) card and the second being the PIN to access the mWallet. Although this might provide more security, it is arduous from the user's point of view since he has to remember two PINs for a single device. Also, the PIN for the mobile device only has to be re-entered if the device was switched off. Given that most mobile devices are not switched off that often, the two levels of authentication practically do not exist if the mobile device is in the active state. MNOs in many countries (India and UK for instance) do not require, by default, the entry of a PIN to access the SIM card in the phone. On switching on the phone, the SIM is automatically activated. The two levels of authentications would obviously not apply to such a case either.

Interestingly, (Dahlberg et al., 2002) mention that mPayment solutions are easy to use given that authorization makes use of two PIN codes with the mobile device. However, this is in comparison to electronic and internet banking. As a payment option, the ease of use of a payment system has to be compared to other payment

options available in the market, especially those that would be favoured over mPayments; these would be credit cards, debit cards and cash. Compared to these, where all that the consumer would have to do is provide a signature or remember a single PIN for the credit/debit card, the two-PIN system is cumbersome.

Other software would include the actual mPayment application. An example of such software is the application used by NGPay. NGPay is an mPayment system used in India. The software is essentially an mWallet with additional functions that aid the customer in managing his payment transactions by maintaining a list of merchants and payment history amongst other features. NGPay is further explained in Chapter 4. Although the software is available for download at any time, these could also be provided by the mobile device manufacturer.

***End-User/Consumer*:** Possibly the most important link in the value chain, the consumer is the entity that eventually uses the mPayment systems. If there aren't enough customers using mPayments, it is unlikely to be successful. The greater the number of users, the more valuable the payment network (Henkel et al., 2002).

Precisely defining and understanding who constitutes the target population is vital for the functioning of any business idea (Hammer et al., 2003). The product has to fulfil the demands of the target group and should be tailored to their likes and dislikes. The entire life-cycle of a product is more or less influenced by this; the branding, the marketing approach and the channels used. All this depends on the target customer. This holds good for mPayments too.

As described earlier, the adoption of the mPayment system by the merchant greatly influences consumer acceptance and vice versa. If the merchant does not see a substantial number of customers using or wanting to use a particular payment system, it is not feasible for him to provide it as a payment option. It can be seen here how the network effect could affect the acceptance of the merchant. Conversely, if the customer cannot use a payment system at a number of merchant establishments, the payment system would not be attractive to him.

2.2.3. The Payment Life-Cycle

(All of the following information referenced from (Ondrus et al., 2004) unless otherwise noted).

The payment life-cycle is discussed here because it illustrates the course of a payment process and, since it gives a better insight to the various players involved in the mPayment scenario, the different roles that they can take on and how they would need to collaborate with each other.

Note that there is a difference between a player and a role. While a role is a set of functions that need to be performed, a player is the entity that performs these functions. Consequently, a single player could take on two roles: the content provider could be the merchant at a POS terminal, a vending machine or an eCommerce service provider. Of importance is to understand how a payment transaction takes place and what the significant steps are in the process.

Figure 1 illustrates the life cycle of a generic payment transaction, which is applicable to any form of electronic payment transactions, including mPayments. This life cycle can be segregated into nine steps.

0. Registration: Before initiating a payment process, the consumer usually has to enrol/register[4] with the payment provider. This encompasses capturing customer information, bank details, the authentication procedure and/or the installation of the required software on the mobile device, if it doesn't exist on the device already.

Downloading an applet or installing the required software does not usually take more than a few minutes. With many mPayment applications – which typically process micro-payments – an explicit enrolment is not carried out. For example, when downloading digital goods like logos and ringtones, there is no explicit enrolment; the first purchase serves as enrolment. The consumer agrees to the terms and conditions of the merchant through his first purchase; an identification or verification process is not carried out and billing is done along with the mobile

[4] In literature, the terms registration and enrolment have been used synonymously. However, registration usually refers to a "smaller" process than enrolment, comparable to the registration of an email account. Enrolment is a more rigorous process. In this thesis, we shall use the term enrolment.

phone bill or the amount is deducted from the prepaid credit available. The actual enrolment is such a case is implicit and automatic.

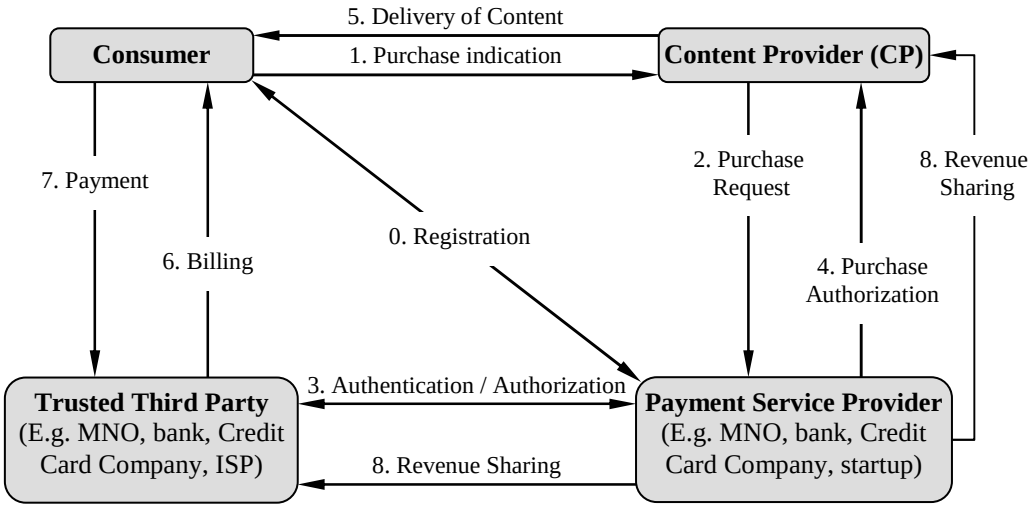


Figure 1 – The Payment Life – Cycle (Ondrus et al., 2004).

From the merchant's point of view or from the view of the payment provider, with monetary values this low, an enrolment process may not be required or may not be feasible given the low risk proposition and the high costs of enrolment. However, considering the fact that a significant percentage of young adults and adolescents in the age group 13-24 – who form the prime target group of downloadable goods – are already in financial debt (Korczak, 2005), the question as to whether some kind of informative enrolment process should be in place does arise, even if it only includes obtaining a consent statement from the parents/guardians of under-aged mobile subscribers.

In most macro payment scenarios, customer enrolment is not just the mere "registration" of the customer for the payment solution, but it also serves as the identification and verification of the person. Enrolment is crucial in the case of any payment process, since all further authentication will be based on the data collected during the enrolment stage; the reduction of fraud being the prime concern. To achieve this, the correct identity of the person has to be established as well as his financial credibility.

After the initial enrolment process, the consumer can start using the payment application to make purchases provided the payment option is offered on the merchant side. (Players: Consumer, Payment Service Provider).

1. Payment Indication: On purchasing an item, the consumer initiates the payment process through the merchant by providing the transaction details consisting of the payment amount, the account number (or mobile phone number which serves as the account number), user identification and some sort of authentication (Players: Consumer, Merchant).

2. Purchase Request: The merchant then requests an authorization from the payment service provider (Players: Merchant, Payment Service Provider).

3. Authentication/Authorization: The payment service provider in turn checks the authenticity of the user with the trusted third party. The trusted third party and the payment service provider could be one and the same player. For instance, in a credit card transaction, the payment service provider would be the merchant acquirer and the trusted third party would be the credit card issuer (Players: Merchant, Payment Service Provider, Trusted Third Party).

4. Purchase Authorization: After establishing the identity of the consumer, the payment service provider authorizes the merchant to carry out the transaction (Players: Merchant, Payment Service Provider).

5. Delivery of Goods: The consumer receives the goods (Players: Merchant, Consumer).

6. Billing: The trusted third party bills the customer. In the case of mPayments, the customer could be billed along with his mobile phone bill, in a separate bill or the amount can be deducted from the customer's bank account (Players: Consumer, Trusted Third Party).

7. Payment: The customer pays the billed amount to the trusted third party (Players: Consumer, Trusted Third Party).

8. Revenue Sharing: The involved players share the revenue obtained (Players: All players involved except for the consumer and merchant).

2.3. The mPayment Value – Chain

(All of the following information referenced from (Contius et al., 2003) unless otherwise noted).

Similar to the payment life-cycle, the mPayment value chain describes the payment process for mPayments in particular, rather than payments in general. Also, this mPayment value chain will be used in Chapter 5 to incorporate biometric authentication.

The mPayment value chain consists of eight core activities illustrated in Figure 2.

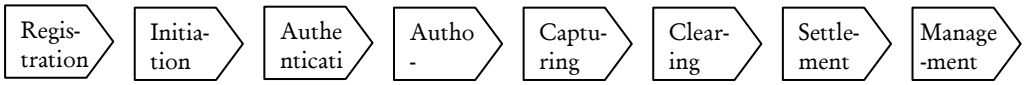


Figure 2 – The mPayment Value Chain (Contius et al., 2003, p. 61)

- The consumer first **registers** for using the payment system. It encompasses all activities starting from customer acquisition up to the enrolment process.

- The payment **initiation** phase is the actual point of transaction when the customer has selected his goods and is now ready to pay. The merchant receives the transaction credentials and has to now check with the payment provider if the transaction can be carried out. This is done in the next two phases.

- The **authentication** phase verifies if the person really is who he claims to be. It checks if the data provided at the time of the transaction and the enrolled data are the same. Usually, payments are authenticated by means of signatures or PINs. It is in this authentication phase that biometrics could potentially be used and is further discussed in Chapter 5.

- After the customer has been authenticated, the payment transaction has to be **authorized**. The authorization phase checks to see if the transaction for the given amount can be carried out. It checks, amongst other things, if the customer is financially covered to make the transaction.

- The **capturing** phase no longer involves the customer. Capturing refers to saving the transaction details in a system database. All data that is required for the billing and settlement phases are captured and stored.

- The **clearing** phase involves the confirmation and transfer of payment instructions mainly between the acquiring bank (bank of the merchant) and the issuing bank (bank of the customer). Banks do not settle funds on an individual transaction basis. They collect together a set of payment instructions for each transaction and perform a batch settlement between each other on a higher level. Once the funds are transferred, the receiving bank then breaks it down to the individual accounts as per the payment instructions.

- **Settlement** is where the funds are actually transferred between the various financial houses involved.

- The final phase in the payment process is **management**. This deals with the consolidation of the customer bill and sending the bill/statement to the customer. It also includes dealing with customers in case of default. Essentially, management encompasses all post-settlement interaction with the customer.

Each of these activities is handled by different players. The actual distribution of roles varies depending on who dominates the value chain. In an MNO-dominated model, for example, the registration and authentication would be carried out by the MNO. Also, the above explained value chain is a simplified form of the mPayment value chain. The mPayment value chain can be complex. Assigning

the best role to each player would require time (Hampe et al., 2003a) and depends on the core competency of each player and their level of involvement.

2.4. The Mobile Payment Reference Model

(This section, unless otherwise mentioned, has been taken from (Pousttchi, 2005))

The Mobile Payment Reference Model (MPRM) is an information model, developed by Pousttchi in his doctoral dissertation (Pousttchi, 2005). The model aims to provide a framework for ubiquitous mPayment and to improve the collaboration between the various players involved. Pousttchi defines the model as "a technically and economically interoperable information model developed to support mPayment processes, especially in the realization of cooperation between the various complementary players involved in the payment procedure." (Pousttchi, 2005, p. 3)[5].

The MPRM consists of two sub-models: the reference organisation model and the reference application system model. The reference organisation model regulates the cooperation between the players, analyses the different possible utilization scenarios for mPayment and maps these scenarios against a few standard mPayment (MP) types. In simple terms, a standard MP type is a grouping of mPayment procedures based on their characteristics and have been derived by (Kreyer et al., 2002). Utilization scenarios can be best described as different situations or application areas where different digital (online articles, downloads like music, ringtones, online books, etc) or non-digital goods can be bought using mPayment. The reference application system model specifies the system view of the MPRM with the help of a semantic model. This system view is comprised of two sub-views: the external view represented by a use-case diagram and a semantic view represented by means of a class diagram. This thesis will not delve

[5] *„…ein technisch und wirtschaftlich interoperables Informationssystem zur Unterstützung mobiler Bezahlvorgänge, das zur Umsetzung einer Allianz komplementärer Anbieter von Bezahlverfahren geeignet ist und durch eine systemimmanente Herstellung dieser Kooperation die Vorraussetzungen dafür schafft, mobiles Bezahlen innerhalb und außerhalb des Mobile Commerce zu einer etablierten und weitverbreiteten Zahlungsart werden zu lassen."(Pousttchi, 2005)*

deeper into the application system model since this part of the model is not relevant to the core subject of this work.

MPRM Organisation Model

The MPRM organisation model has been developed by analysing different possible utilization scenarios for mPayments and by mapping these against a selected set of three standard MP types. (Kreyer et al., 2002) arrived at a total of five different standard MP types: three of these are used by the MPRM organisation model. For the sake of understanding, the three standard types used by the organisation model are explained after the description of the utilization scenarios.

The Cartesian product obtained from mapping the utilization scenarios against the three derived standard MP types give a set of 21 possible combinations (a given payment type used in a given payment scenario). From these combinations, the most promising and valid combinations are extracted and form the organisation model.

Utilization scenarios

The utilization scenarios are differentiated based on the type of goods purchased – digital or non-digital – in either mCommerce, eCommerce or in regular brick and mortar commerce; additionally, it includes the payment transfers from customer-to-customer (C2C). This gives a total of seven different utilization scenarios, which are summarized below:

A – Purchase of digital goods in mCommerce against a premium charge
B – Purchase of digital goods in mCommerce against a fixed charge
C – Purchase of digital goods in eCommerce
D – Purchase of non-digital goods in eCommerce or mCommerce
E – Purchase of goods from a vending machine
F – Purchase of goods at POS
G – C2C Payment transfer

Standard MP Types

Standard Type I is a standard type where mPayment billing is done along with the phone bill and where the settlement is done by the MNO. Since the MNO already bills the customer for airtime, transaction costs in this regard are relatively low. As this type is a post-paid standard type, the risk involved is higher as there is no cap to the amount the consumer could spend using the mPayment application. One way of reducing this risk is by having an upper "spend threshold" within the mPayment application itself. Needless to say, there is also the risk of fraud in case the mobile device gets into wrong hands.

Standard Type II, on the other hand, is a bank-centric standard type meaning that settlement is done by the bank and functions through a direct debit system or a credit card transaction. Again, this is a post-paid standard type; however, it generally does not bear the risk that standard type I comes with since the amount of the transaction is indirectly capped by the amount of money in the consumer's account – in case of a direct debit transaction, or the credit limit if using a credit card.

Both standard type I and II together are not universally applicable. To ensure universality, (Pousttchi, 2005) introduces **standard type III,** based on the prepaid standard type. The customer stores a monetary value on his mobile device and uses it to make his payments. There are no strict rules with regard to the amount. One idea is to aggregate smaller amounts together and to settle it as a standard type II settlement once it reaches a certain threshold value. The characteristic features of the three derived standard types are summarized in Figure 3.

Figure 3 indicates that the authentication techniques suggested for the different standard types are the conventional mobile device authentication systems. In the case of micro-payments, there is no authentication process per se; the user is only identified by means of the Mobile Subscriber Integrated Services Digital Network (MSISDN) number. This would mean that anybody who has access to the mobile device could initiate a payment. One could argue saying that in the case of micro-payments the amount is so low that the costs involved in making the system more secure are far higher than the corresponding risk of fraud. However, an mPayment

application that is perceived to have a high level of security is more likely to be accepted than one with a lower level of perceived security. Having a well secured mPayment application also means that it will be secure enough for macro-payments as well.

	MNO/Bank Centric Type	Transaction Costs	Security Level	Authentication Method	Type of Payment
Standard Type I	MNO-centric	Low	Medium	Via MSISDN	Micro (Postpaid)
Standard Type II	Bank-centric	High	High	PIN Authentication	Macro (Postpaid)
Standard Type III	Bank-centric	Low	Medium	PIN/MSISDN	Micro/Macro (Prepaid)

Figure 3 – Characteristic features of the derived standard types (Based on (Pousttchi, 2005))

From the set of values obtained from the Cartesian product, valid combinations are extracted. A valid combination is the application of a standard MP type in a given utilization scenario where the implementation is theoretically and practically possible and well-suited for the involved players. Since the mainstream of this thesis does not concentrate on the MPRM model, the method and reasoning for the derivation of the valid combinations will not be discussed in detail. AS example of how a valid combination is derived is given below. Of interest is mainly the result which is given in Figure 4. The Cartesian product gives a total of 15 valid combinations, which are denoted by “X”.

To illustrate how these combinations have been derived, the utilization scenario “E” and its derived combinations are explained here. Scenario “E” is a scenario where non-digital goods are purchased at a POS vending machine. Such a payment situation would not necessarily be ideal for an MNO-centric application. Standard type I is not suitable for vending machines due to the receivable margin, the possibility of reclamation in case of a machine defect and the high probability that vending machines are in areas that have a weak mobile signal. Standard type III would here be an apt payment type since it can handle both macro and micropayments. Standard type II also is a possible payment type in scenario “E”.

The combinations given in parentheses () indicate that either type can be used. For example, in the utilization scenario “C”, apart from type II, either type I or type III can also be included.

Utilization Scenario	Standard MP Type I	Standard MP Type II	Standard MP Type III
A	X		
B	X	X	
C	(X)	X	(X)
D	(X)	X	(X)
E		X	X
F		X	X
G		X	X

Figure 4 – Cartesian Product of utilization scenarios and standard types (Based on (Pousttchi, 2005)

These 15 possible combinations form the MPRM organisation model. Interestingly, no single standard type can be used in all utilization scenarios. To ensure an ubiquitous mPayment application, a permutation of two standard types would have to be used. Coupling standard type I and II or I and III would cover all utilization scenarios.

The MPRM organisation model also regulates the cooperation between the various players in the payment process by stipulating which player is best-suited to handle the payment process in a certain scenario. Such a regulation gives a kind of guideline for vertical as well as horizontal alliances. A vertical alliance is the cooperation between the same kind of player; for instance the cooperation between MNOs would be a vertical alliance. A horizontal alliance is the cooperation between players with complementary players like banks and MNOs. Figure 5 illustrates the horizontal and vertical alliances between banks and MNOs.

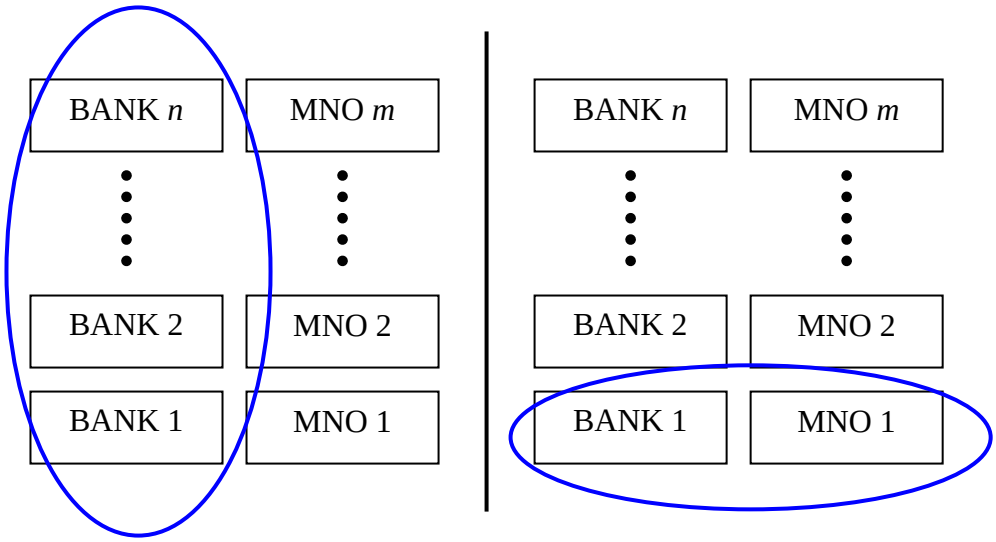


Figure 5 – Vertical and Horizontal Alliances between Banks and MNOs (Pousttchi, 2005, p. 37)

Both vertical and horizontal alliances contribute to making the mPayment application ubiquitous and standardized. Users have their mobile subscriptions with various MNOs, their credit card with different issuers and their bank accounts with various banks. The horizontal and vertical alliances would ensure that the mPayment application is available to as vast a user base as possible. The larger the number of banks and MNOs in the alliance, the larger the covered user base. NTT DoCoMo in Japan is a perfect example of how alliances between a numerous of players can ensure a successful mPayment application. NTT DoCoMo is described in Chapter 4.

2.5. Contemporary Security in mPayments

Security in the digital world has become a major concern with issues like data privacy gaining more and more weight. Digital services, in particular mobile services, can only be successful if the user perceives the system to be secure and thereby trusts the system enough to use it (Rannenberg et al., 2005). When it comes to a payment system, the security requirements are all the more vital. In a study conducted by (Krueger, 2004) only 15.8% of approximately 13,000

respondents found paying through a mobile device to be secure. Of interest is also a study conducted by (Wiedemann et al., 2008). In this study, the respondents were asked if they would be willing to enrol to use an mPayment application and if yes, in how many: only 8.2% of users said that they would not enrol in an mPayment system. While this may not directly reflect what the users think about mPayment security, it can be deduced that the respondents would not contemplate enrolling in a system they did not perceive as secure. The study analyzed 1123 filled out questionnaires; two-thirds of the respondents were a "tech-savvy" population. Given this, the percentage numbers may not be representative of the general public.

The Oxford dictionary defines security as *"the state of being or feeling secure"*. Applying this to payments, a secure payment would be one in where the actual transaction is secured against all sorts of fraudulent and privacy attacks and one where the consumer feels secure about using the payment application. A payment system can be considered as secure if it satisfies the five payment security features.

2.5.1. Payment Security Features

There are five features to security in an electronic transaction. These are authentication, confidentiality, encryption, data integrity and non-repudiation (Hampe et al., 2003a).

Authentication: Authentication refers to the ability to uniquely identify the parties involved in a transaction and to determine the validity of this identity (Creese et al., 2003). In a payment transaction, it is important that both the customer and the merchant are authenticated (Dannenberg et al., 2004) since both are equally prone to fraudulent attacks. While the merchant could be faced with a fraudulent customer with a stolen identity, the customer could be faced with a fake merchant through attacks such as phishing. Phishing is a method of attempting identity theft, where the offender sends out emails pretending to be a merchant or the user's bank and requests personal data from the user such as his password or banking details. This often involves misdirecting the user to a site

that looks like the merchant's or the bank's official site. Although phishing is more predominant on the internet, it is slowly finding its way to the mobile world, too (Chellam, 2005).

Confidentiality: Confidentiality refers to the user identity and user information being kept concealed (Dannenberg et al., 2004). In any payment transaction, data pertaining to the customer like his address, the purchased item and probably the credit card details or bank account details are collected. While this information is necessary to carry out the transaction, the collected data should not be disclosed to any third party unless legally required to do so. It should be used only in context with the payment. Confidentiality of the data should be maintained not only during the transmission but also when it is stored. In many situations of identity theft, stolen credit card details and similar kind of frauds, it is not during transmission of the data that the information is stolen, but by hacking into the central repository where this data is stored.

Encryption: The safe transmission of data requires it to be encrypted. Encryption means that the data is encoded and cannot be read/ deciphered without the key to decrypt it. This ensures that data transmitted cannot be tapped during the transmission, which is vital in an mPayment situation where the payment details have to be transmitted.

Data Integrity: Data integrity means that the data cannot be modified in any way by unauthorized persons. The data should be transmitted to the merchant and from the merchant to the payment provider in the same state as it left the customer. The data should be protected from intentional as well as unintentional attacks (Dannenberg et al., 2004).

Non-Repudiation: Non-repudiation is the assurance that the financial transfer has taken place. Non-repudiation is necessary to ensure that neither the sender nor the receiver can deny having sent/received the data, or in the case of mPayments the money. This non-repudiation of the end-user is of great significance to merchants/vendors (Hampe et al., 2000), since it ensures that they receive their payment.

Ensuring that these five features are met would mean that the following questions are answered:

- **Is the customer who he claims to be?**
- **Is the merchant who he claims to be?**
- **Is my data in the right hands? Will it be passed to a third person?**
- **Can my data be read during transmission?**
- **Has the merchant received my payment?**

Assuring these five security features also increases the trust of the customer in the payment system. Knowing that the money reaches the right person, that the data is kept both safe and secure and that the payment is carried out with no problem would possibly remove all doubt from the consumer's mind.

2.5.2. Authentication – The Key Security Issue

Authenticating a user can be done in numerous ways like using passwords, PINs, smart cards or tokens. Based on the method used, authentication can be divided as follows (Bolle et al., 2004; Currie, 2003):

(i) **Knowledge-based authentication (K):** Something the user knows like PINs and passwords.

(ii) **Object-based authentication (P):** Something the user owns like smart cards or tokens.

(iii) **Biometric-based authentication (B):** Something the user possesses like measurable personal traits of the user.

The differentiating properties of these authentication methods are given in Figure 6.

Method	Examples	Properties
What you have **(P)**	User IDs, ATM Cards, Keys, Badges	*Can be shared* *Can be duplicated* *May be lost or stolen*
What you know **(K)**	Passwords, PINs, Personal knowledge	*Many passwords are easy to guess* *Can be shared* *May be forgotten*
What you are/ unique personal trait **(B)**	Fingerprint Face, Iris Voice print	*Not possible to share* *Repudiation unlikely* *Forging is difficult* *Cannot be stolen or lost*

Figure 6 – Summary of authentication types (Based on (Bolle et al., 2004))

In many cases, you make use of a combination of knowledge and possession as in the case of using an ATM with the ATM card and a PIN (Bolle et al., 2004). Here, the plastic card is the object the consumer has and the PIN is the knowledge he possesses. An identification card with the biometric feature of the person embedded in them would be:

(P, B) => (ID, Fingerprint)

Here, the user has his ID, which is something he possesses, and it makes use of the user's biometrics, which is a part of the user.

The current most widely spread authentication form is the usage of PINs (Nanavati et al., 2002). By force of habit or merely having no other choice, most consumers have become accustomed to PINs. In many mPayment systems, authentication takes place within the mobile device usually by entering the PIN. When using a mobile device, there is a clear identification of the user as he enters the PIN to access the SIM card and thereby more security than when using debit cards or credit cards which require only a signature. Forging a signature is far simpler than cracking a PIN (Henkel, 2001b).

PINs can be a secure mode of authentication if the PINs are long enough and complicated enough so that they cannot be cracked; but this is rarely enforced as such PINs are difficult to remember. This in turn might cause user to write them down, thereby bringing back the security to almost null (Rila, 2002).

Authentication can also be provided by biometric methods. As mentioned in Chapter 1, biometric authentication refers to the automated use of unique human characteristics to verify a person. There are quite a few advantages that make biometrics better than PINs. The key advantages of biometrics over knowledge and token-based authentication techniques are that biometric characteristics cannot be forgotten like a password, or lost like a key (Currie, 2003; Rila, 2002); nor can they be stolen or given willingly to another person. Also, the fact that biometric authentication information is non-transferable makes it powerful against repudiation (Rila, 2002).

Effective authentication is the central activity within the mPayment value chain (Contius et al., 2003). Ensuring that only the rightful owner has the ability to use a given payment system would increase the trust the customer has in the security of the system. Also, ensuring good authentication would minimize fraudulent usage of a payment system, thereby reducing the risk factor for the merchant and the payment provider. Hence, ensuring that there is an authentication process in place that the user is comfortable with, that the user trusts as secure enough is an important factor for any mPayment application.

Since authentication has been established as a key factor in mPayments, the choice of which authentication method should be used to ensure a safe payment environment arises. Of the three methods of authentication, token-based authentication does not qualify for use with mPayments since it requires the user to carry an additional item on him, which defeats one of the purposes of using mPayment, namely the reduction/elimination of carrying cards, cash or other items for payment utilization. This leaves us with biometric-based and knowledge-based authentication. As knowledge-based authentication methods are widely in use today, it has been decided to explore the possibilities of using

biometric-based authentication in mPayment systems. The main reasons for this are the advantages that biometric authentication has over knowledge-based authentication. PINs can be forgotten, shared and are easy to guess. Users nowadays are subject to remembering PINs for various applications – their cards, the mobile SIM, phone banking etc. This can lead to the user getting confused between the various PINs or forgetting them. Biometrics on the other hand are always on the person and are almost never subject to change. They are unique and cannot be easily forged. Therefore, biometrics seem to be a more secure option than PINs as they satisfy the 5 security features better than PINs; additionally, they are more convenient to use than PINs since the user does not need to remember anything. The reason why biometrics are chosen is discussed in detail in Chapter 3; the chapter will also deal with identifying a biometric that would be best-suited for use in mPayments.

3. Identifying a Biometric for mPayment Systems

Identifying people by means of their physical and behavioural characteristics is used everyday by everyone (Nanavati et al., 2002). We recognize people by their face; on the phone we are able to identify people we know based on their voice. Sometimes, we are even able to recognize the people we know by the way they walk. This kind of manual recognition however is not biometric recognition: biometrics is the **automated** recognition of people based on their physical or behavioural characteristics.

Biometrics are finding their way into different fields as a means of establishing secure identification and authentication as described in Chapter 1. Early adopters of biometrics were government agencies and the military (RCMP, 2002). Today, biometrics are used in relatively trivial applications, such as securing laptops, to more conscientious applications like citizen ID cards, airport security (see Chapter 1 for examples) and even a few isolated payment applications like digiPROOF, which is described in Chapter 4.

This chapter will describe:

- why biometrics could be considered as an authentication method in mPayments and
- given the various biometric methods available, filter out the biometric methods most suitable for mPayment applications.

3.1. The Basics of Biometrics

To identify a suitable mPayment biometric, a basic understanding of the biometric subject matter is required. This includes the definition of biometrics, how the consumer's biometric data is captured, defining how biometric accuracy is measured, and differentiating between identification and verification.

3.1.1. Definition

(Nanavati et al., 2002, p. 9) define biometrics as the *"automated use of physiological or behavioural characteristics to determine or verify identity."*

A more detailed definition is given by (Bolle et al., 2004, p. 3) who say: *"Biometrics refers to identifying an individual based on his or her distinguishing characteristics. More precisely, biometrics is the science of identifying or verifying the identity of a person based on physiological or behavioural characteristics"*.

Both these definitions encompass two essential aspects of biometric differentiation: behavioural versus physiological biometrics and biometric identification versus biometric verification. These are explained in the next two sections respectively.

3.1.2. Categories of Biometrics

Biometric methods can be classified into two basic types – behavioural and physiological. There is also a third derived type namely combined biometrics. These three types are explained below.

Behavioural Biometrics: Biometric methods that identify or verify persons based on aspects of their behaviour are known as behavioural biometrics. It requires the active participation of the person being authenticated (Wolf et al., 2003). They are based on the characteristics of a certain action that is performed by an individual. For example, signature verification measures factors like the writing speed, the pressure used and time taken. These actions have a clear beginning and a clear end and therefore occur in a certain time-frame. *"The element of time is essential to behavioural biometrics"* (Nanavati et al., 2002, p. 10). Whatever is measured in the given time-frame forms the biometric pattern. Behavioural biometrics are dynamic and can change with the passage of time. They are further characterized by external factors like the environment and education. Handwriting for instance, and consequently the signature are influenced by the schooling the writer had and the personalized style that the writer adds to it and can vary with age.

Physiological biometrics: When the physical features of a person like the eye, finger or skin are assessed for unique characteristics, the biometric method is termed as a physiological biometric. The physiology of a person remains more or less unchanged throughout his lifetime, unless affected by accidents or other wear and tear incidents. These are static features that the person is born with and that are not influenced by external factors. Iris scanning, retina scanning, hand geometry, fingerprint reading and face recognition are different biometric methods based on the physiological characteristics of a person.

Combined Biometrics: Some biometrics make use of both the physical traits as well as the behavioural characteristics of a person. These are called combined biometrics and assess the physical characteristics of the body based on their behavioural elements. One such combined biometric is speaker recognition. Speaker recognition uses physiological elements like the vocal tract, the nasal cavities and the modulation of the human as well as behavioural elements like the accent and the pronunciation of the speaker (Nanavati et al., 2002). The latter are defined by environmental factors like the place where the person grew up and the kind of education received. These are characteristics that evolve over the years and can change. However, the physical aspects like the vocal tract, tongue and the nasal cavities remain the same.

A combined biometric that is commonly used with payments is signature verification. Credit cards, debit cards and cheques use signature verification. Legal documents, contracts and identification documents like passports all bear the signature of the person for establishing the identity. Driving licenses, passports, identity cards and other forms of personal documents bear the photograph of the holder. There are also credit cards with the photo of the owner on it so as to minimize fraud (Bank of America, 2009). Behavioural and physiological characteristics are used by everyone to identify people in day-to-day life. When we speak to someone over the phone or see people we know on the road, we instantly recognize them based on their voice and face respectively. The difference is that these processes are all manual forms of identification/verification. Biometric methods or technologies as Nanavati refers to them are automated processes that use technological devices to carry out the

authentication process. It is only a biometric authentication when the process is assisted by a system that makes the authentication decision. For example, if a forensic investigator visually matches fingerprints, it is not a biometric authentication. On the other hand, if an automated reader is used to match the fingerprints and takes a real-time decision, then the system is performing a biometric authentication (Nanavati et al., 2002).

Apart from the above types of biometrics into physiological, behavioural or combined, a biometric can also classified based on when/how the underlying human trait was developed: a ***genotypic*** biometric is one where the biometric trait is defined by genetics; face recognition would be a genotypic biometric. A ***phenotypic*** biometric is one where the trait is formed when the human being is still in the embryo stage. Also referred to as *randotypic* biometrics, examples of this type are fingerprints and iris patterns. ***Behavioural*** traits are those that are learned over the years like signature verification or speaker recognition (speaker recognition is also a genotypic biometric to a certain extent - a combination of both) (Fried, 2007)[6].

3.1.3. Reasons for using Biometrics

Given the fact that current authentication processes seem to function without any issues, the question as to *why* these present methods need to be replaced or complemented by biometrics methods surfaces. Stated below are the reasons why biometrics are used in general, and why biometrics could be used in mPayments in particular[7].

1. **Security:** The key advantage that biometrics has over knowledge and token-based authentication techniques are that biometric characteristics cannot be forgotten like a password, or lost like a key (Currie, 2003; Nanavati et al., 2002; Rila, 2002). The use of biometrics can reduce the possibility of fraudulent usage of the mobile device in general and the mPayment application in particular. The use of biometrics in mPayments

[6] Paragraph on biometric traits referred from (Fried, 2007)
[7] Point 1 to 3 are primarily taken from (Nanavati et al., 2002) while Point 4 is referenced from (Rila, 2002).

could also aid in increasing the user's perception of how secure the mPayment application is.

2. **Convenience:** Biometrics eliminate the need for remembering tedious passwords or carrying around token-based security items. This makes it considerably convenient for the customer when compared to knowledge-based or object-based authentication systems. For an mPayment user, the same factors of convenience apply. Activating an mPayment application using a biometric is much simpler than entering a PIN code especially when waiting to pay at a POS terminal.

3. **Increased Accountability:** Using biometrics to authenticate persons eliminates buddy-punching systems (Nanavati et al., 2002) since the biometric cannot be transferred to another person. It also helps to accurately keep track of the when the customer used the payment application last. Such kind of an auditing often serves as a deterrent to fraudulent activities.

4. **Non-repudiation:** The fact that biometric authentication information is non-transferable makes it powerful against repudiation (Rila, 2002). Using biometrics in mPayments ensures that the user cannot deny having initiated the payment. Since the biometric is bound to a person, no one else could have initiated the payment. This factor should actually make mPayment an attractive mode of payment for merchants to offer.

Nevertheless, biometrics has its problems as well. Although it cannot be lost in the literal sense, the human body can be damaged through accidents thus causing the biometric characteristic to be "lost" or be mismatched with the enrolled biometric template. What can also be done is that a reprint of the biometric is taken every few years. The enrolled biometric template could be given an "expiry date" like credit cards, where the user has to re-enrol himself to continue the usage. This would again cause a rise in costs. There should be relevant backup authentication methods in place should the biometric authentication process not work.

3.1.4. Identification Vs. Verification

(Bolle et al., 2004, p. 17) define authentication as *"the process of reliably determining the identity of a communicating party"*. It is essentially the process of establishing who a given person is. Authentication is a process that involves both identification and verification. While identification answers the question "Who is he?" verification answers the question "Is he Mr. X?" where Mr. X is the claimed identity. For example, when a person withdraws money from the ATM, his card is used to identify him. Here, the account number is read from the card and is then compared to all account numbers in the database, till a match is found. This is identification. After the user has been identified, he is asked to enter his PIN, which is checked against the one associated with the identified account number. This is verification. Now that the person has been authenticated, he is free to continue with his banking issues. These same concepts of identification, verification and authentication are extended to biometrics as well.

Identification is more time-consuming as well as a more difficult biometric process when compared to verification. When biometrically identifying a person, the biometric template is matched against all templates in the database to find out who the person is. In other words, a **1:N matching** takes place (Nanavati et al., 2002). A 1:N matching is a one-to-many matching where 'N' is the number of database records. Given the value of **N**, this matching process can take a very long time since a decision (Match or No – Match) has to be made for each and every template in the database.

During verification on the other hand, the identity of the person is already established by some other distinct means. The biometric template only serves the purpose of validating this identity. Quoting (Furui, 1996), *"the fundamental difference between identification and verification is the number of decision alternatives"*. Verification matches the one live template against the one template stored for the established identity. It is a **1:1 matching** (Nanavati et al., 2002) where there are only two decision alternatives and where only a single decision needs to be taken.

Between a 1:1 and a 1:N matching, there is also a 1:few (one-to-few) matching method. Here, the template is matched against a small group of known users (Nanavati et al., 2002) to identify the person. The number of users may range from as few as five to as many as a hundred users. There is no clear distinction as to when a 1:few matching becomes a 1:N matching. For the scope of this thesis, we will concentrate on the verification process as we are looking to use biometrics for the verification process in mPayment.

3.1.5. Biometric Performance Metrics

Several performance metrics are used in order to assess the accuracy of a biometric. These performance metrics provide the possible proportion of error that a biometric is capable of. On matching a live template with a stored template, the resulting decision – a "Match" or a "Non-Match" – could be correct or erroneous. For instance, a false person could be given a "Match" or an authentic person could be given a "Non-Match" (Bolle et al., 2004); these are both erroneous decisions. The estimation of these erroneous matches made is given by the False Acceptance Rate (FAR) and by the False Rejection Rate (FRR).

The Equal Error Rate (EER), Failure-to-Enrol Rate (FTE), Failure-to-Acquire Rate, the Ability-to-Verify Rate (ATV) complete the list of performance metrics and are all described below. All these values, unless otherwise specified, are percentage values.

False Acceptance Rate: The FAR is the *probability* that an impostor is identified/verified as somebody he is not (Nanavati et al., 2002). FAR is also referred to as False Match Rate (FMR). An ideal situation would be where the FAR is equal to 0%. However, in practice, this is very unlikely. The lower the FAR for a given biometric, the less the biometric is prone to fraud.

The FAR as stated above is referred to as the single FAR; it is the rate indicative of a single comparison. There is also a system FAR which is the likelihood of an impostor breaking into a given system as opposed to breaking through a single person's biometric. According to (Nanavati et al., 2002), the system FAR is far

more important in practical applications than the single FAR. The system FAR is dependent on the single FAR, the number of attempts a user has before the system bars the user and the number of identities that the impostor has access to, amongst others (Nanavati et al., 2002).

False Rejection Rate: Otherwise known as the False Non-Match Rate (FNMR), the FRR expresses the likelihood that an authentic individual is rejected by the system (Ashbourn, 2004). FRR usually occurs when the live template and the stored template are inconsistent. The reasons for this are summarized by (Nanavati et al., 2002) as follows:

- *Changes in the user's biometric data:* Due to possible wear and tear, the physical characteristics of a person could be altered. For instance, a bad cold could affect the voiceprint of the user; a small cut on the finger would alter the fingerprint. Also, over time, the behavioural characteristics of a person could change. As a person grows older, his handwriting may change.

- *Difference in how the user presents biometric data:* The way the user presents his biometric data could vary each time and more importantly vary from how he presented it during enrolment. Differences in pressure when placing a finger on the biometric reader, differing volume when recording the voiceprint are examples of such a difference.

- *Changes in the environment in which the data is presented:* This can be a common cause for a high FRR since enrolment is usually carried out in a closed environment which does not reflect the actual live environment where the user would be presenting his biometric. For example, when using speaker recognition, background noise could result in the user not being verified.

FRR is a classic case of "Denial of Access" (Rila, 2002); something which is far more damaging in a payment environment than FAR from the viewpoint of customer retention. Being denied access to his own money could be annoying –

and also embarrassing – to the customer. Given a scenario in a restaurant where the customer tries to pay and is not able to because the system falsely rejects him, is similar to being labelled an impostor from the customer's viewpoint since it could leave the impression that he is not sufficiently covered financially. Such an experience would lead to customer dissatisfaction with the used technology and could, as a result, potentially lead to losing the customer.

Failure-to-Enrol Rate: FTE represents the probability that a user cannot enrol in a given biometric system. This can be the case when the user's biometric characteristic is not sufficiently distinctive or replicable or when the chosen biometric solution is more prone to a high FTE than others (Nanavati et al., 2002).

Gathering ample biometric data can help reduce the FTE. For example, capturing a number of prints of the same finger or capturing a longer voiceprint can be helpful to enrol a user. Further reduction of the FTE can be achieved by a supervised enrolment process where the user is guided by trained personnel and taught how to authenticate himself in real-life applications.

Equal Error Rate: The EER is derived from the FAR and the FRR. Commonly used to represent the overall accuracy of the system, EER is the rate at which FAR and FRR are equal to each other (Nanavati et al., 2002). This means that the likelihood of allowing an impostor access to a system and denying an authentic person is the same. (Nanavati et al., 2002) continues to say that the EER is rarely used as a guideline when implementing a biometric system since it is quite a misleading rate. It does not include the FTE rate and therefore does not correctly reflect the performance of a biometric system although it combines the FAR and the FRR.

Ability-to-Verify Rate: ATV is a combination of the FTE and the FRR. It gives *"the overall percentage of the users who will be capable of authenticating on a daily basis"* (Nanavati et al., 2002). ATV is of interest to this thesis since it is a decisive factor that influences the costs, security and convenience of a biometric system (Nanavati et al., 2002).

For the sake of completion, all metrics have been explained above. However, the most important metrics that are usually used to judge a system's accuracy are the FAR, the FRR, the FTE and the ATV. However, these metrics do not reflect the exact accuracy of a biometric system. They only give an estimation of the probability that an error will occur (Bolle et al., 2004).

Ideally, the FRR should also be as close to zero value as possible. However, this too, is not possible in practice. The FAR and the FRR are inversely proportional to each other, meaning that as one decreases, the other increases (Nanavati et al., 2002). This is because biometric authentication uses a threshold value. The threshold is a numerical value based on which the match-non-match decision is made. If the result of the matching process which compares the reference template and the live template is above the threshold value, then it is a match; if it is below the threshold it is a non-match (Nanavati et al., 2002).

The FAR and FRR are dependent on the threshold value. The higher the threshold value, the lower the FAR, which is good; this prevents fraudsters from being accepted by the system and making it more secure. However, a high threshold would mean the probability that a genuine person is rejected is higher. This is because "*the nature of biometric data is such that two different measurements of the same biometric feature from the same person are very likely to be different*" (Rila, 2002, p. 21). The slightest difference in the way the user presents his data, background noise, dirt, etc could all cause the rejection of a genuine user. Inversely, the lower the threshold value, the more likely it is for an impostor to break the system. A balance between the two should be sought; or depending on the kind of security required, either the FAR or the FRR should be given more importance, indirectly taking into account that either impostors are accepted or that authentic users are denied access.

3.2. Using Biometrics in MPayment Systems

In a set of interviews conducted by (Mallat et al., 2003), the results showed that one of the risks consumers see with mPayment is that an unauthorized person would be able to pay with their mPayment application in case of loss or theft of

the mobile device. Using biometrics instead of present authentication techniques could possibly eliminate this fear altogether.

In terms of implementation, biometrics can be easily employed in mPayments. Depending on the type of biometric used, only a small hardware device needs to be added to the mobile device. If using speaker recognition, even this would not be necessary, since the microphone which is required for speaker recognition is already present in all mobile devices. For fingerprint recognition, a small reader would have to be fitted into the mobile device. There are already mobile phones fitted with fingerprint sensors. On research, the earliest model that could be found was the Korean company Pantech's GI100 which was launched in 2004[8]. In 2006, Pantech launched a follow-up model, the PG 6200 in Asia and the USA[9]; this phone is shown in Figure 7. Interestingly, the PG 6200 also has voice recognition capabilities.

In 2008, the laptop company Lenovo introduced their first mobile phone, the P620, with a fingerprint sensor[10]. In January 2009, NTT DOCOMO launched the Fujitsu F-01A mobile phone with fingerprint technology from AuthenTec[11], which is supposed to be waterproof as well. All these phones use fingerprint recognition to "unlock" the phone. This means that only the owner is able to use the phone.

There are also a few payment applications that use biometric authentication. Mobilkom Austria and ekey biometric systems had launched a project where visitors could buy tickets to the Ars Electronica Festival 2001 using mPayments secured by fingerprint recognition (ekey Biometric Systems, 2001). Although not an mPayment application, in parts of Germany consumers are able to buy products at their local supermarket using fingerprint verification through DigiPROOF. DigiPROOF is further described in Chapter 4.

[8] (Fiutak, 2004)
[9] (www.inside-handy.de, 2006)
[10] (www.chip.de, 2008)
[11] (www.gsmdome.com, 2009)

Figure 7 – The Pantech PG 6200 with an Integrated Fingerprint Sensor (PC Welt, 2006)

Not all biometrics are suitable for use in mPayments. Not all biometrics can be used with mPayments. Small mobile devices dictate the size of the biometric reader to be small; to the players, the costs involved will also be a decisive factor. The following section examines what factors should be considered when selecting a biometric for use in mPayment applications and devise a criteria catalogue. Once the criteria catalogue has been established, the possible biometric alternatives will be examined.

3.2.1. Selecting a Biometric – The Criteria Catalogue

To select a biometric best-suited for mPayments, a set of criteria were established based on factors that are of significance to mobile telephony and payment. These criteria serve to compare the different kinds of biometrics and in the process, to find out which one is best suited for mPayments. On a high level, these criteria have been classified as *technical factors, security, business factors* and *consumer acceptance*.

Technical Factors

The **device size** of the biometric reader should be small enough to fit into the mobile device. Mobile devices today are becoming smaller and smaller and if the size of the biometric reader impacts the overall device size, it would possibly not be attractive to the consumer who looks for his mobile device to be as small as possible.

The **size of the biometric template** should be small enough not to take up too much memory space if stored on the mobile device. Although today's mobile devices have powerful processors and sufficient storage capacities, the prime use of the mobile device is not payment; hence, the space used for template storage should not interfere with any other functions of the mobile device.

Another factor is the **technical reliability** of the biometric (Teletrust e.V., 2002). Technical reliability would mean that the hardware used to read the biometric and the software that processes it function consistently.
The chosen biometric should be **robust** and able to perform accurately under all circumstances. External factors like background noise, dirt, heat or humidity shouldn't affect the system.

Security Factors

The **accuracy** of the biometric used is paramount in the choice of the biometric. This accuracy is determined by the performance metrics which were discussed in Section 3.1.5. The accuracy of the biometric greatly depends on the threshold value and the quality of the enrolment process.

The chosen biometric must be **secure**. This security is dual-fold; not only must the biometric secure the data it is protecting, but the biometric data, namely the template, needs to be secure (Teletrust e.V., 2002) in terms of the five security factors described in Chapter 2. Security in this context refers to how secure the biometric template is. It should neither be easy to forge the template, nor should it be possible to circumvent the biometric and gain access to the data it protects.

Business Factors

Using biometrics should be **cost-effective** for all parties involved and especially for the customer. The biometric-based mPayment system should be cost-effective enough that the customer chooses it over other payment options. The more expensive the implemented hardware in the mobile device, the more expensive the device becomes, which in turn would deter the consumer from trying out the device. The merchant should also not incur any additional costs for offering the payment system as an alternate payment option. Changes to the existing payment infrastructure at the merchant's POS should be minimal. Obviously, to ensure a better profit margin, the payment system needs to be as cost-effective as possible to the payment provider as well.

Response time is another significant criterion to be considered. Response time refers to the time taken to authenticate the consumer. It is *"the time required to measure the human characteristic in order to create the template and the storing time of the template"* (Royal Canadian Mounted Police, 2002). The response time starts at the initiation phase of the payment life-cycle discussed in Chapter 2 and ends with the payment authorization after which the consumer receives his goods. This whole process should ideally not take more than a few seconds. A normal card transaction takes around 10 – 15 seconds. Given this, an mPayment transaction using biometric authentication should not exceed the same time. Longer response times, even if only by a few seconds, can make the process seem time-consuming and can annoy the customer.

The process of **enrolment** should also be taken into consideration when deciding which biometric to choose for mobile devices. For example, a tedious enrolment process might not be feasible for a micro-payment application. However, a detailed enrolment can improve the accuracy of the chosen biometric.

Factors affecting Consumer Acceptance

For the customer to use a new technical system, it needs to be **user-friendly**. Biometrics like iris-scanning and retina reading tend to be rather user-"unfriendly" since it requires the user to look into an object, which can be a bit

awkward. This could make him uncomfortable and not very keen on using the system.

The **ergonomics** of the biometric device plays an important role in customer acceptance (Teletrust e.V., 2002). The biometric should be convenient and intuitive to use without making him feel that it is too technical.

Main Criteria	**Characteristics**	
Technical Factors	Reliability	*Does this biometric perform consistently?*
	Robustness	*Is the biometric resistant to external factors?*
	Device Size	*Is the biometric device small enough to fit mobile devices?*
	Template Size	*Is the size of the biometric template suitable for use in mobile devices?*
Security Factors	Template Security	*How secure is the biometric template from hackers? Can it be forged?*
	Accuracy	*Is the biometric accurate enough for usage in a payment application?*
Business Factors	Costs	*Would it be economic to use the biometric?*
	Response time	*How quickly can the transaction be carried out with this biometric?*
	Enrolment	*How difficult is enrolment going to be?*
Consumer Acceptance Factors	User-friendliness	*Is the authentication process self-explanatory?*
	Convenience	*Is the biometric easy to use for the consumer?*
	Ergonomics	*Is the biometric device human-engineered?*
	User Perception	*What does the user think about the biometric?*

Figure 8 – The Criteria Catalogue

Another factor influencing customer acceptance is the **user perception** of the biometric (UK Biometrics Working Group, 2002). Fingerprint verification, for instance, is easily associated with criminal records and therefore, users may not be comfortable using this as a verification technique.

All these factors sum up to form the criteria catalogue depicted in Figure 8. In the next section, this criteria catalogue is applied to a set of possible biometrics to evaluate which biometric would be best-suited for use in mPayments.

3.2.2. Selecting a Biometric – Possible Alternatives

This section aims at using the criteria catalogue derived in Section 3.2.1 to identify a biometric suitable for use with mPayments.

As mentioned earlier, the size of the biometric reader plays a very important role in choosing a biometric for mPayments. For simplicity, the author has already made a pre-selection and filtered out biometrics whose device sizes make it impossible for usage with mobile devices. Such biometrics that have been eliminated from the evaluation are hand geometry, DNA analysis, keystroke pattern and gait recognition. The biometric methods that have been considered for mPayments are:

1. Signature Verification
2. Fingerprint Verification
3. Face Recognition
4. Iris Recognition
5. Speaker Recognition

1. **Signature Verification:** Signature verification is a behavioural biometric that analyses the signature of the person. It is a behavioural biometric that evaluates a person's handwriting, the pressure applied while writing, the time taken, etc.

   Signature verification is divided into static and dynamic signature verification. Usually the signature is captured on normal paper and then either scanned or photographed and digitized for comparison (Schmidt et al., 2001). Static signature verification only analyses the signature print/image; the actual process of signing is not analysed. Dynamic signature verification on the other

hand, verifies the active movements involved in signing like the total time taken, the speed and the pressure to name a few (Schmidt et al., 2001).

Given the lack of constancy in a person's signature (when the same person writes the same word twice, it tends to differ), signature verification is not very reliable (Schmidt et al., 2001). The reliability of the signature depends heavily on user behaviour. On a positive note, signature verification is robust and is not greatly affected by external factors. All it requires is the person to sign. Signature verification would require special devices like an instrumented pen and digitised graphics table (Schmidt et al., 2001), which could be too expensive to be feasible for such an application. Signature verification may be possible when using PDAs, but even in this case, it is not really reliable since the use of a touch screen instead of a writing pad affects the quality of the signature (Koreman et al., 2006).

Signature verification does not provide a very high level of security as a signature can be easily forged. Dynamic signature verification is more fool-proof than the static version, but when compared to other biometrics, security is still low. The accuracy is also far from desirable with the FAR and the FRR values being too high (Scheuermann et al., 2000). (Kholmatov et al., 2005) conducted a study where they analysed the FAR and FRR for signature verification. Depending on the classifier used, the FRR ranged between 1.64% and 3.60%; the FAR ranged between 1.28% and 3.52%.

The enrolment process does not largely vary from that of other biometric methods. To gain a representative signature template, multiple instances of the signature have to be captured during enrolment, which would be the case for a few other biometric methods too as described below. The advantage that enrolment for signature verification has over other biometric methods is that the user is accustomed to signing and hence will be more at ease with the system. Also, enrolment could theoretically be carried out at any location. Almost no additional equipment is required. The response time for signature verification is only 1 millisecond (Jansen, 2003), which is also very good.

Although not as a biometric verification system, consumers have been using their signatures in connection with payment systems like cheques, credit cards and debit cards for a long time and therefore the user perceives it as a safe authentication method. It is user-friendly and convenient. When it comes to the ergonomics too, the user would not have any problem either since he is used to writing and the signature is given almost unconsciously (Schmidt et al., 2001).

Signature verification would qualify in many aspects for use with mPayments. It has an excellent response time, consumer acceptance is good, it is robust to external factors and has a small template size. However, given that not all mobile devices work with a graphic tablet and come with a special pen, it may just not be feasible to equip the devices with these as this would not only drive up costs, but also make it uncomfortable to the user if he didn't want a device with a digitized pen. Moreover, signatures tend to be easily forgeable, especially when using the static version and it is not reliable since two different versions of a signature from the same user can differ. Given all these issues, signature verification may not be suitable for authentication in mPayments.

2. **Fingerprint verification:** Fingerprint verification is the earliest biometric to be used and the first computer-aided personal identification system (O'Gorman, 1999). It functions by reading the pattern on the upper third of the finger. This pattern is made up of whorls, loops and arches, which are the primary types of fingerprints.

   Fingerprint authentication as used in commercial applications differs greatly from the Automated Fingerprint Identification System (AFIS) used by law enforcement agencies for forensic investigations (Royal Canadian Mounted Police, 2002) – a fact that the general consumer is not aware of. The AFIS uses high-quality black and white images of the fingerprint (and not templates) and compares these to fingerprint images in a database to filter out potential matches. These are then scrutinized by a fingerprint expert (Royal Canadian Mounted Police, 2002). On the other hand, fingerprint

verification/identification uses a fingerprint template that is reduced to the minimal details required to authenticate a person. AFIS captures the entire fingerprint and the image therefore has a size of up to 250 Kbytes; the fingerprint template is smaller by a factor of 250 to 1000 (Behrens et al., 2001). Most important of all, a fingerprint as used in payments cannot be easily restored from the reference template. Communicating this to the customer could alleviate any apprehension that the customer may have about using fingerprint technology and contribute to consumer acceptance.

The greatest advantage of fingerprints is that no two people have the same fingerprint and that the fingerprint doesn't change over time (Behrens et al., 2001). This makes fingerprints very reliable. However, this reliability is subject to user behaviour. Variations in the style of placing the finger on the reader could affect the reliability of the method. Reliable as it may be, fingerprint verification is unfortunately not very robust as it is susceptible to lower performance due to environmental aspects like dirt or grime on the reader or the user's fingers.

As can be seen in Figure 7, fingerprint sensors today are small enough to fit into mobile devices. Therefore, the size of the reader is not an issue here. The size of the fingerprint template is relatively small as well ranging between 40 and 256 bytes (Jansen, 2003).

The fingerprint template that is stored is secure in the sense that the original print cannot be reproduced from the minutia data of the template (Jansen, 2003); this is because the stored template is a highly extracted version that contains only the most essential features required for comparison with the live template. Also, fingerprint verification is a very accurate biometric when compared to the other biometric methods in consideration for mPayments. It has very low FAR and FRR rates (Hassler, 2001).

In terms of costs, fingerprint sensors are more affordable in comparison to other biometric sensors. According to (O'Gorman, 1999), a biometric sensor could be obtained for around 100$ a piece back then. This number is almost

ten years old and given that cost of technology falls with time, the cost of fingerprint sensors would be comparatively less today. At the time of writing this thesis, the author was not able to find substantial, reliable evidence to back the cost of sensors. This was of course the retail price, mobile device manufacturers would buy a large quantity at a much lower price.

Fingerprint verification has a very good response time. According to (Chung et al., 2005), the response time only takes a few seconds. The enrolment process tends to be quite tedious for fingerprint verification. To ensure a high recognition rate, the enrolment process needs to produce a high quality template (O'Gorman, 1999, p. 13). For best results, the same finger would have to be enrolled a number of times to ensure a reduced FAR. However, this would also bring up the FRR, if the user does not present his finger the same way during the live capture.

Fingerprint verification is a technique that the user needs to get used to. Per se, it is user-friendly and convenient in the sense that all the user has to do is place his finger on the sensor. The actual authentication process is easy to understand as well. Depending on how and where the sensor is embedded within the mobile device, the sensor would be easy to access as well. The main disadvantage of fingerprint verification is the user's perception of it; he associates fingerprint verification with criminality (Ng-Kruelle et al., 2005). The general user does not differentiate between the AFIS and biometric fingerprint verification and hence may not be comfortable giving their fingerprint because of the criminal stigma related to it.

Despite all the disadvantages, fingerprint verification could be a potential biometric verification method that could be used with mPayments. The factors that speak for this are the size and cost of the sensor, the accuracy, the resistance to forgery and the response time. Mobile devices with fingerprint sensors can already be found on the market and since fingerprint reading is slowly finding its way into other commercial as well as government applications, fingerprint verification might lose the criminal stigma that the user associates with it.

3. **Face Recognition:** The easiest way for any person to be recognized is by looking at his face. In its simplest non-biometric form – using photographs – face recognition is used in many areas like passports, IDs, driver's license and even on credit cards. Face recognition is quite simple to use (Bolle et al., 2004) since all that needs to be done is capture a picture of the user. Traditional face recognition functions by measuring the distances and angles between a geometric point in the face like eye corners, mouth extremities, nostrils and the chin. Some facial recognition applications also makes use of intensity patches like the cheek intensity and that of hair as well as eye region patches (Weng et al., 1999). In the case of authentication in mPayments, face recognition would be carried out in a controlled environment since a single person needs to be verified and not identified. There are two types of face recognition; the first is face recognition in a "controlled environment", where the person is known and there is not much change in the environment, like directly photographing a person at a constant distance. The second type is the "random environment" where the person is anywhere in a camera scene (Ashbourn, 2000).

   Since most mobile devices today have an in-built camera, taking a facial photograph should not be all that difficult. (Hazen et al., 2003; Koreman et al., 2006) have tried securing PDAs with voice recognition, face recognition as well as signature verification proving that theoretically face recognition can be used with mPayments and on mobile devices. However, the quality and resolution of the built-in cameras in mobile devices are not sufficient to be used for face recognition. According to (Bolle et al., 2004), regular camera footage is not really useful for face recognition due to the low spatial resolution. Therefore, to use face recognition, powerful cameras/ sensors need to be built into mobile devices. This causes an increase in costs. Accuracy in facial recognition is also not all that good (Bolle et al., 2004; Thiel, 2002). Problems like changes in physical appearance and lighting lead to high recognition error rates. For example, differentiating between identical twins (Bolle et al., 2004) or verifying a man's identity even after he grows a beard still pose problems.

The reliability of face recognition is far from desirable. Performance is not consistent when people wear glasses, grow a beard or make other changes to their appearance. Although no scientific information has been found to this effect, cameras are generally usable in all weather conditions and are not affected by other external factors. However, face recognition requires a clear background whilst taking the picture. Background noise by other people, designs on walls etc. make face recognition difficult since the actual body to be authenticated cannot be differentiated from the background. In a payment scenario, this is often the case – be it in a retail store or if the customer is at home and shopping over the internet. Face recognition would therefore not classify as a robust biometric.

Mobile phones today have 5-8 mega pixel cameras built into them, which means that these cameras would suffice to produce a good quality image for verification purposes. The latest mobile phone from Sony Ericsson (Sony Ericsson C905) has an 8.1 mega-pixel camera. In an experiment conducted by (Hazen et al., 2003), a 640x480 CCD camera was used, which is a 0.3 mega pixel camera , to capture an image for face recognition. In the experiment, the image was transferred to remote servers for face detection due to the current computation and memory limitations of the mobile device. This experiment was conducted for speaker identification and face identification rather than verification. It is known that the verification process requires less computational powers than the identification process and in terms of memory would need only enough memory to store the template. Therefore, in the verification process, we may not have to transmit the data to a remote server for processing. Coming to the template size, the face template bears a size of approximately 500 bytes (Hassler, 2001, p. 381), which is bigger than the template size of other biometrics under consideration.

Research shows that face recognition has an acceptance rate between 1% and 2% and a rejection rate that lies between 10% and 43% (Hassler, 2001; Phillips et al., 2000). Again, these numbers are ten years old and given the advancement of technology, these values would probably have improved over

time. The high rejection rates could be attributed to the appearance of people changing over time. Changes in hairstyle, glasses and ageing could also affect these metrics.

No data with regard to response time was found. However, considering that a lot of care has to be taken when taking the picture (positioning in front of the camera, watching the angle etc), the total time taken to complete the payment transaction would be long even if the response time of the actual verification process is very small. The costs involved in terms of hardware are minimal since most mobile devices have cameras that are qualitatively good enough for face recognition. The enrolment process is not as tedious as when compared to fingerprint verification or speaker recognition. A single image taken in front of an adequate background is sufficient.

Although people are used to looking into cameras, taking a picture when they are standing at the POS is not very comfortable and is also time-consuming. It is not exactly user-friendly for an mPayment application. It is also not convenient to use: using the built-in cameras of mobile devices to take your own picture is not very easy to do, since the image being taken cannot be seen. A plus point that face recognition has is user perception. Users are willing to use face recognition since it is the most natural form of identification (Polemi, 1997).

4. **Iris Recognition:** The iris is supposed to be a universal biometric identifier, which has good discriminating properties. It does not change with age (Bolle et al., 2004). The iris is the coloured part of the eye, which surrounds the pupil and which is bounded by the sclera (white tissue of the eye). The iris of every human being is so unique that even the left and right iris patterns are different (Ashbourn, 2000). The advantages of iris recognition are that it is very resistant to false matching and hence one of the most accurate biometrics available. It also has a very good response time, taking less than a second to authenticate the user (Daugman, 1999).

Though iris recognition is a very accurate biometric technique, it is also very expensive (Thiel, 2002). Also, the calculation used in the production of the IrisCode are quite advanced and the necessary processing capacity in not yet available in the common mobile device (Eriksson, 2001). It is however very secure, accurate and very resistant to false matching (International Biometric Group, 2005). The user has to present his head in a very precise location and stare into the camera for a few seconds with eyes wide open. (Royal Canadian Mounted Police, 2002) which does not make it very user-friendly and convenient for a quick payment at check-out. Enrolment is also difficult because of the associated discomfort (Royal Canadian Mounted Police, 2002). It may not be compatible with mobile phones due to its size, and is relatively expensive (Royal Canadian Mounted Police, 2002) when compared to other biometrics. The size of the template is usually between 256-1000 bytes (Hassler, 2001).

The above-mentioned factors itself disqualify iris recognition from use in mPayments, not to mention problems with the hardware required for iris recognition.

5. **Speaker Recognition:** Speaker recognition is otherwise also known as voice recognition or voice scan. Speaker recognition functions by authenticating the user based on his voice. It measures both the behavioural as well as the physiological characteristics (Nanavati et al., 2002) associated with the voice of a person like the accent and intonation as well as the pitch, intensity and frequency (Nanavati et al., 2002).

   Speaker recognition is just one of the various speech processing techniques. There are also speech synthesis, speech recognition, speech coding and language recognition (Hampe, 2004 (Lecture)). It often happens that speaker recognition is confused with speech recognition (Nanavati et al., 2002). While speaker recognition identifies the voice and consequently the speaker, speech recognition identifies the words that the speaker says.

   With reference to mPayment, speaker recognition involves fewer costs when compared to other biometrics. This is because speaker recognition only

requires a microphone to capture the voice and this already exists in all mobile devices, thus eliminating the problem of device size as well. The only major additional requirement would be the software that compares the two voiceprints (templates). Speaker recognition is also very user-friendly since the user does not have to learn anything new – all he has to do is speak into his phone, which he is used to doing. The only negative criterion is the accuracy of speaker recognition. According to (Hassler, 2001), speaker recognition has a FAR and FRR of 1% each, which is higher than that of the other biometrics. The accuracy however, can be improved by proper enrolment and by setting the right threshold value for comparison. Also, according to (Nanavati et al., 2002), certain speaker recognition technologies are highly resistant to impostor attacks, even more than fingerprint verification.

Speaker recognition is not all that reliable though. Changes in the speaker's voice – both short-term and long-term – can affect the live template. A cold, fatigue or a sore throat can alter the voice just like age does over time. The emotional state of the user can also alter the live voiceprint (Bolle et al., 2004). When it comes to robustness, the performance of speaker recognition is subject to external factors like background noise (Zinke, 2001). The device size does not pose a problem since the microphone required is already embedded in the mobile device.

Depending on the level of detail, the template size can range between 100-1000 bytes. Enrolment can be quite tedious as in the case of fingerprint verification. To obtain the voiceprint, the speaker would have to give multiple samples of his voice.

Speaker recognition is user-friendly as speaking is the most natural thing for a user to do. It is also convenient in the sense that the user already speaks into the phone and would therefore not be doing anything new. However, some people might find it uncomfortable authenticating themselves using speaker recognition in a public environment, like for example at a POS terminal. The user might want to keep the payment process discreet and authenticating himself loudly might be awkward to him. Since the primary function of most

mobile devices is telephony, the devices are usually made ergonomically for this function. Speaker recognition has a greater likelihood of being accepted be the user since it does not have the negative perceptions that are associated with other biometrics (Nanavati et al., 2002).

From the above, it can be seen that speaker recognition could also potentially be used in conjunction with mPayments. The low costs, affinity to telephony, natural characteristic and relatively good accuracy make it ideal for authentication purposes in mPayments.

	Signature Verification	Fingerprint Verification	Face Recognition	Iris Recognition	Speaker Recognition
Reliability	3	4	2	5	1
Robustness	5	3	2	4	1
Device Size	1	3	4	2	5
Template Size	3	5	1	2	4
Template Security	1	4	3	5	2
Accuracy	3	4	2	5	1
Costs	2	3	4	1	5
Response Time	3	4	2	1	5
Enrolment	5	4	2	1	3
User-friendliness	5	3	2	1	4
Convenience	5	3	2	1	4
Ergonomics	3	4	2	1	5
User Perception	4	1	3	2	5
TOTAL	43	**45**	31	31	**45**

Figure 9 – Applying the Criteria Catalogue to selected Biometrics

Figure 9 plots the different criteria from the criteria catalogue against the short-listed biometric authentication techniques. The table uses a simple scoring system where it ranks the criteria on a scale of 1 to 5 with respect to usage in mobile devices, with 5 being the highest score. The biometric with the highest score is the one that will be chosen for use in mPayments. From

Figure 9, two possible biometric methods could be selected for authentication purposes in mPayments. These are **Fingerprint Verification** and **Speaker Recognition**. The biggest advantage that speaker recognition has is its low costs, which makes it the best method for use in telephony. However, users might find it uncomfortable to speak into his phone at the POS whilst there are others queued up behind him. The low accuracy might also require the user to speak into the phone a number of times. Additionally, it has to be decided what exactly the user is to say into the phone for recognition. It cannot be a set PIN or password since people around him would hear the spoken code. An alternate is to use PINs that are randomly generated for each transaction. This results in additional computational costs.

Fingerprint verification on the other hand, is more practical and discreet, making it easier and convenient for the customer to use. No additional PINs have to be generated and accuracy is better than speaker recognition meaning that the user would not require as many attempts to get authenticated. Going further in this thesis, the author has decided to use **fingerprint verification** as the best authentication method for mPayments, but at the same time draw parallels to **speaker recognition** as well. Since the enrolment process for both these technologies are equally complicated, the major differentiation factor would be cost and user acceptance.

4. The Market Picture – A Look at Different Continents

Many mPayment applications have been introduced worldwide over the last few years. This chapter provides an overview of the mPayment market scenario and gives an insight to individual biometric payment systems around the world. Although an effort to cover all continents has been made, emphasis has been given to Asia and Europe. For each continent, a selected set of countries have been chosen. The choice of countries was based on the progress/success of mPayment applications in that country. Factors that were taken into consideration were the widespread use of the application, consumer acceptance and the ability of the application to withstand the test of time. Germany, India and the UK were chosen based on the geographic location and background of the author.

On an application level, the players, the type of payment and the target group of the mPayment application have been illustrated. However most importantly, an attempt has been made to explain the enrolment process, the required infrastructure and the authentication process. An exception to this description model has been made in the case of Japan. This is because Japan, a country which could be seen as a pioneer in the field of mobile applications, uses a standard payment platform called “Osaifu-Keitai”. A vast set of payment providers use this platform and base their mPayment applications on it.

Different countries are in different phases of development with reference to the market penetration of mPayments (Karlsson et al., 2006, p. 77). This idea can also be extended to customer acceptance, and sophistication of the application. Asia as a whole is by far the market leader amongst all continents when it comes to well-established mPayment applications; according to Ondrus, Japan, Singapore and Korea are the leaders in the mPayment market as they have mPayment applications that can be used in all the different transaction environments (Ondrus et al., 2009) that are described in Chapter 2

A further attempt has been made to address a wide range of areas where mPayment can be applied. From the described applications, it can be seen that

mPayments are used in the fields of transportation, for online transactions, as well as parking amongst others.

4.1. Asia

Asia can boast of many mPayment applications that are widely used by a large customer base. In a report, (Gartner Inc., 2008) mentions that Asia is the market leader in mPayments with approximately 28 million users, Japan being the local leader.

4.1.1. Japan

Japan has always been an interesting market for the mobile industry. From the days of i-mode[12], Japan has always had a strong affinity to adopt the latest in mobile devices and mobile phone applications.

Japan has a population of around 127 million people as of 2008. Around 87% of these are mobile subscribers, which is higher than the percentage of internet users at around 71% and PSTN subscribers at 37% (International Telecommunication Unit, 2008). Interestingly the percentage of mobile subscribers has been steadily increasing over the last 12 years, from approximately 4 million in 1995 to over 1 billion in 2007, while the number of landline subscriptions has gone down from around 800,000 in 1995 to approximately 360,000 in 2007 (Statistics Bureau Japan, 2007)

Japan has come a long way in terms of mobile technology with the latest innovation being *"Osaifu-Keitai"*[13]. Founded in 2004, Osaifu-Keitai literally means "wallet mobile" (Wikipedia, 2007). However, it differentiates itself from conventional mobile wallets because it uses contactless Radio Frequency Identification (RFID) technology and can therefore be used as a multi-purpose mobile wallet containing cash, credit cards and debit cards, as well as other utility cards such as membership cards and ID cards. It can further be used to buy and

[12] I-mode was introduced in Japan in February 1999. For more information, see (Hampe et al., 2000) and http://www.nttdocomo.co.jp/english/service/imode/
[13] Entire section, unless otherwise mentioned, referenced from (NTT DOCOMO, 2008)

store travel tickets and hold access cards or keys. Applications using the Osaifu-Keitai are the best examples of proximity payment applications.

Osaifu-Keitai has become something like an mPayment standard platform in Japan on which many mPayment applications as well as other mobile applications are based. Not only are there many vendors that are equipped to process Osaifu-Keitai transactions, but it is also supported by different mobile operators despite being developed by NTT DoCoMo. This makes it highly accessible to almost all mobile phone subscribers in Japan; this is the perfect example of how vertical and horizontal alliances between the players involved contribute to the success of the mPayment application as mentioned in Chapter 2. There are over 30 applications that are based on/make use of Osaifu-Keitai. A few of the mPayment applications are described below. The mobile devices need to be equipped with the Osaifu-Keitai platform, which includes Felica's RFID technology. Apart from this, no additional infrastructure is required.

Edy

Edy is a prepaid payment service provided by Bit-wallet Inc.[14] in Japan. The name Edy stands for **E**uro, **D**ollar, **Y**en (Skinner, 2008) – a potential indication that the payment providers intended it to become an international mPayment solution. As of now, Edy is only available in conjunction with the Yen.

Edy works on NTT DoCoMo's Osaifu-Keitai platform. As mentioned earlier, Osaifu-Keitai has evolved into a standard mPayment platform for multiple mPayment applications; all mobile operators offer phones that are Osaifu-Keitai enabled. Given this, Edy is available to all customers who have a mobile device with Osaifu-Keitai. Since it has been adopted as a standard platform, other providers like Softbank and Au also provide phones equipped with Osaifu-Keitai.

How It Works: According to the Edy website (www.edy.jp, 2008)[15], as of September 2008, there are about 79,000 merchants and branches who accept Edy

[14] BitWallet Inc. is a company co-founded by Sony and NTT DoCoMo, amongst others, in 2001 offering ePayment solutions (Hagiu, 2006)
[15] Translated from the Japanese using Google's translation service.

as a form of payment. These include convenience stores, super-markets, drug-stores, department stores and even amusement parks (www.edy.jp, 2008).

Paying with Edy is fairly simple. When wanting to pay, the merchant activates the Edy sensor and the customer simply places the mobile device in close proximity to the sensor, making sure that the RFID tag faces the Edy sensor. The payment amount is then deducted from the balance stored in the Osaifu-Keitai wallet.

Topping up the Edy account can be done either at the POS terminal in selected stores offering the Edy payment facility or at charging machines. This is done via the RFID interface, too. The amount is paid to the merchant and the amount is credited to the Edy wallet. The wallet has a storage limit of 50,000 Yen (approximately 320€) and in a single top-up transaction a maximum of 25,000 Yen (approximately 160€) can be credited to the wallet.

Players Involved: To make Edy work, a number of players are involved. The primary player is bitWallet, who is the payment provider for Edy. Since the Osaifu-Keitai platform is provided by NTT DoCoMo, the company can also be considered as one of the major players. The list of indirect players would include Sony who provide the RFID interface in the form of Felica, mobile phone manufacturers who include the Osaifu-Keitai during the manufacturing process as well as the carriers, Au and Softbank mobile, for instance. An essential success factor in the Edy business model is the cooperation between all these players. Additionally, other MNOs like Au and Softbank offer Edy compatible phones since they too utilize the Osaifu-Keitai platform. Users would only need to install the application.

Enrolment: There isn't really much of a process involved in enrolling for Edy. If the mobile device does not come with Edy installed – as is the case with all carriers except for NTT DoCoMo – the user has to install the application. This can be done through the Edy website, where a barcode is available. Scanning the barcode installs the application on the mobile device (www.edy.jp, 2008).

After this, Edy has to be activated before it can be used. No checks are performed and no personal information is gathered at any stage. The user accepts the terms and conditions set forth by Edy with the click of a button and the account is activated. A serial number (Edy number/Edy ID) is then assigned to the mobile device, which functions as the account number. In case of theft or phone loss/defect, the amount stored in Edy can be recovered using this number[16].

JCB's QUICPay

QUICPay is a mobile credit card service offered by the Japan Credit Bureau (JCB International) – a Japanese credit card company (JCB International, 2004).

How It Works: With QUICPay the credit card details are stored in the Osaifu-Keitai. A part of the customer's credit limit is assigned to the Osaifu-Keitai mobile wallet (JCB International, 2004). QUICPay functions through the contactless RFID tag – Felica – that the Osaifu-Keitai phones are equipped with. It effectively works the same way as Edy does, with the difference being: instead of the total payment amount being deducted from the wallet, on payment the credit card details and the assigned credit limit is read from the wallet and the amount is charged to the credit card account of the customer. The entire transaction works offline with no connection to the credit card provider being necessary since the credit limit is read from the wallet. According to (JCB International, 2004), the total time taken for a transaction is less than a second; all the customer has to do is hold the phone close to the POS reader. This would make it quicker than a cash transaction.

Players Involved: Apart from the constant players involved in any Osaifu-Keitai payment application, there is also the mPayment provider namely JCB. Here too, the collaboration between all players involved is vital to be able to provide the payment.

Enrolment: There is no explicit enrolment process, for existing customers. An application to use QUICPay can be made either through the mobile device or

[16] (www.coolstuffjapan.sblorgh.org, 2007)

online. A credit check is performed and the user is provided with an ID. The user is now ready to use his mobile credit card (OMC Card Inc., 2006).

Mobile Suica

Mobile Suica is an mPayment application, again based on the Osaifu-Keitai, and is offered by the East Japan Railway Company for its customers to pay for their travel tickets. It was introduced in January, 2006. The Suica system is a prepaid fare card where the customer keeps a prepaid balance in his keitai phone. It is the mobile equivalent of the stored fare card that the railway company offers (NTT DOCOMO, 2008). Apart from the train services offered by the JR East, the mobile pass can also be used on buses and the subway[17].

How it works: Like all Osaifu–Keitai applications, Mobile Suica is also a "touch and go" application. Transport services in Tokyo make use of the barrier gate system wherein passengers need to validate their tickets before they get to the platform or onto the train. This system ensures that a person does not have access to the platforms without a valid ticket. Some of these fare gates are equipped with sensors capable of reading the data from the mobile device. On entering and exiting through these gates, the passenger has to "touch in" and "touch out" at the sensor and the correct amount is deducted from the prepaid fare amount (East Japan Railway Company, 2005).

The prepaid amount can be recharged through the mobile device itself. There are two forms of the mobile Suica – one is for those who own a Suica-compatible credit card and the other is for passengers without a credit card. The latter is called "easy-mobile Suica"[18].

To recharge an easy-mobile Suica, the user would have to go to a convenience store that accepts Suica[19]. For a credit card-based Suica, the passenger can recharge his Suica account from the mobile device itself using the Suica menu.

[17] (www.coolstuffjapan.sblorgh.org, 2007)
[18] (www.coolstuffjapan.sblorgh.org, 2007)
[19] (www.coolstuffjapan.sblorgh.org, 2007)

A major advantage of the Mobile Suica is that the money stored in it can also be used to make purchases at select stores (East Japan Railway Company, 2005). Since early 2007, Edy, QUICPay, NTT DoCoMo's ID and Suica have started using a common reader for their mPayment applications as well, making it easier for merchants to offer any of these payment facilities without investing in multiple readers (East Japan Railway Company, 2006).

Players Involved: Apart from the regular Osaifu-Keitai players, the one additional player is the East Japan Railway Company.

Enrolment: The enrolment process for Mobile Suica is not as simple as the registration process for the other Osaifu-Keitai applications described above. To start with, the user has to register on the Mobile Suica website. This includes providing your details and selecting your phone type and your MNO/MVNO. After this, the mobile device scans the barcode form the website. This will open the mobile version of the website through which the user can now download the required applet[20]. Once the application has been installed, the user can logon and enter his credit card details if using the credit card version of the application.

4.1.2. Singapore

With a population of approximately 4.6 million, Singapore has a mobile penetration rate of over 138% (International Telecommunication Unit, 2008). Clearly, there are more mobile subscriptions than the population indicating more than 1 mobile device per inhabitant in some cases. Comparatively, only around 40% of the population are PSTN subscribers and approximately only 73% of internet users (International Telecommunication Unit, 2008). Some of the mPayment applications in use in Singapore are described below.

mNETS[21]

mNETS is an mPayment application launched jointly by the payment provider Network for Electronic Transfers, the MVNO Singtel and the United Overseas Bank (UOB). It completed its 6 month trial run on the February 23, 2009. A

[20] (www.coolstuffjapan.sblorgh.org, 2007)
[21] All information, unless otherwise mentioned, from (www.nets.com.sg, 2008)

selected set of 250 UOB credit card consumers were requested to test the application. mNETS makes use of a mobile wallet and NFC technology to provide the payment facility.

How It Works: To make a payment, the consumer simply flashes the mobile device over the NETS FlashPay reader. mNETS works similar to the Suica recharge scheme, where the consumer tops up his mobile account using his credit card. During the trial period, a total of 500 merchants across Singapore accepted mNETS payments. These merchants can also offer their consumers discounts in the form of mobile coupons.

Players Involved: The only players involved in the trial were 500 merchants, the MVNO SingTel, UOB as the bank, the mobile device manufacturer Nokia and the payment provider NETS. It could well be that once the application is available to the broader public, that there will be more banks and MVNOs involved. Although the trial ended in February 2009, no data could be found as to whether the system was still in use and open to the public.
With regard to providing coupons, there are a few more players involved like Singapore Polytechnic, NXP and ViVOTech.

Enrolment: For the trial, there was no explicit enrolment process. The provider selected 250 UOB credit card users who were given the NFC enabled Nokia 6131 phone. They were not charged any fees and the credit limit was dependent on their current credit status with the bank.

4.1.3. India

India has a population of approximately 1.2 billion people in 2008. According to statistics published by the ITU, 29% of the population are mobile phone subscribers. As a comparison, only around 7% are internet users with only 0.45% owning an internet connection at home. In India, mobile devices and mobile telephony costs are becoming more and more affordable with the passage of time.

The mobile industry in India is quickly growing with plenty of value-added services being offered. Interestingly, this mobile population does not restrict itself

to the urban population or the higher income group. A lot of low income, so-called "single-man businesses" have mobile phones to help them with their businesses: carpenters, electricians etc. all rely on mobile phones so that they are reachable at all times for their customers. For instance, fishermen in the south Indian state of Kerala use their mobile phones to contact ports soon after they've made their catch, they decide on the spot which port to land their fish in depending on the price quoted by each port for their fish (Roche, 2002).

Although the general usage of mobile devices is fast catching up amongst the different demographic groups of the population, there are very few mPayment applications in India. Three successful ones are ngpay, mChek and payMate which are described below. There are also applications for mobile ticketing making their way into the market.

ngpay[22]

Ngpay is an mPayment service developed by JiGrahak Mobility Solutions and provides a method of paying remotely with your mobile device. Essentially, it eliminates the necessity of carrying payment cards. Ngpay is a mobile wallet which stores your payment card details, list of merchants and maintains a history of your payment transactions. Payment details are transmitted via SMS messaging.

How It Works: Ngpay can be installed onto the mobile device either by entering the mobile phone number on the ngpay website – www.ngpay.com – or by sending an SMS message to the providers; in both cases, a link will be sent to the mobile device using with the application can be installed.

Ngpay can be used to make payments to any of the associated merchants. As mentioned earlier, ngpay is a form of remote payment meaning that the customer is not physically at the POS terminal. It is mostly used to make payments for internet/mobile transactions. It can be used to pay for travel tickets, for booking

[22] All information, unless otherwise mentioned, from (JiGrahak Mobility Solutions, 2008)

movie tickets, online shopping with select merchants and to pay general utility bills like electricity, gas, water and mobile phone bills.

One of the significant merchants that provide ngpay is Air Deccan (now part of the Kingfisher airline group). Air Deccan is India's pioneer low-cost airline. Using ngpay, customers can book their tickets directly over their mobile device. All they have to do is choose Air Deccan from their list of merchants/services and then follow the on-screen instructions to make the booking. For payment, the customer can use the credit card saved in the mobile wallet or enter a new one.

Figure 10 – Enrolling for ngpay and the ngpay Wallet

Another large merchant is Sifymall.com. Sifymall is an online shopping portal that offers all kinds of goods to customers from books to electronics and apparels to health & fitness products.

Players Involved: The main players in the ngpay business model is the provider JiGrahak and the merchants ready to accept ngpay transactions. To utilize ngpay, the payment providers assume that the customer is already in possession of a credit card. There is no direct tie-up between the credit card provider and the mPayment provider.

Enrolment: Enrolment/registration takes place just after the application has been installed on the mobile device. The user has to provide details like his name and address. He is also required to choose a 6-digit PIN for security reasons. This PIN

has to be entered each time the user wishes to make a payment using ngpay. Although the PIN does provide the adequate level of security, it is cumbersome to remember a 6 digit number and to enter it each time the user wishes to use his mPayment application. The enrolment screen and the ngpay wallet are shown in Figure 10.

mChek[23]

mChek is an mPayment solution based on SMS technology and offered by the Indian MNO, Airtel. Again, this is another mPayment scenario which in essence gets rid of the necessity to carry around plastic cards and stores the card details in the mobile device instead. Like ngpay, it can be used to pay mobile bills, movie tickets, airline tickets and to pay insurance premiums as well as buy bus tickets.

How It Works: mChek requires the customer to send an SMS message containing the amount to be paid along with the purchase details. For instance, to pay his mobile phone bill the customer would send an SMS message to the provider with the following details: **"PAY AIRTEL <AMOUNT>".** The customer will then be prompted to enter his 6-digit PIN to authenticate himself. On successful transmission of the payment, the customer receives a confirmation SMS message, thereby completing the transaction. The amount is then billed towards the customer's credit card account and the customer settles the dues with his card company/bank.

One of the disadvantages is that mChek is currently only available to Airtel customers. Also, unlike other mobile wallets like the Osaifu-Keitai, only one credit card can be linked to a mobile number. This therefore, does not necessarily eliminate plastic cards from the customer's physical wallet. Finally, the merchant base is still very meagre and therefore does not give the customer ample choice or reason to switch to using the mPayment variation. In other words, the customer would not see adequate value-add to embrace the new payment type when all he can use it for is with a handful of merchants.

[23] All information, unless otherwise mentioned, from (www.mchek.com, 2008)

A major advantage that mChek has is that a vast majority of mobile users are well-versed in the usage of SMS messaging. This makes it easier for them to accept the new mPayment technology as they are already accustomed to sending SMS messages and know how it works.

mChek won the global GSMA 2008 Award for best mobile billing/customer care solution (GSMA, 2008) .

Players Involved: The active players in this kind of a payment solution are the solution-providing MNO and the merchants. The MNO is Airtel and the banks involved are the ICICI Bank, the HDFC Bank, NDB Bank, and the State Bank of India. Visa International and MasterCard are passive players. The banks and credit card companies play a more passive role, since from their perspective there isn't much of a change. They would bill the customer as usual. Interestingly, this would also mean that in case of fraud, it would be the bank/credit card company that would have to bear the losses as would be the case with any normal credit card transaction.

In time, mChek could possibly expand to include customers from different MNOs; this would be vital to reach a larger customer base.

Enrolment: The user can register either on the mChek website or by sending an SMS message to the number specified by Airtel. If using the website, the user enters his mobile number and receives a temporary PIN sent to him via SMS messaging. The customer then creates his own 6-digit PIN and registers his credit card details. On successful registration, the user receives a confirmation message.

As can be seen, there is no explicit security authentication process during the enrolment procedure. It is as simple as setting up an online email account. However, given that the mPayment solution is only available to Airtel customers, there is an implicit level of trust and security as a certain level of background checks would have been done when registering the user as an Airtel customer.

mChek is supposed to make paying bills easier. With mChek, a customer could also pay the bills of other mobile phones belonging to other family members for instance. The test within the SMS message would only have to be modified adequately to reflect this.

PayMate[24]

PayMate works by linking the customer's credit card, debit card or bank account to the mobile phone. The advantage PayMate has over mChek is that it is more convenient as it allows multiple cards to be registered with a single mobile number and is not restricted to customers of a single MNO.

How It Works: PayMate can be used to pay bills, at retail stores as well as for purchases made over the internet. When wanting to make a payment online, the customer would choose PayMate as the payment type and then enter his mobile number when prompted to do so. The customer then receives an Interactive Voice Response (IVR) call from PayMate requesting him to enter his 4 digit PIN to authenticate himself; the PIN is set up during enrolment. Once this is done, the payment is processed and if successful, the customer receives an SMS confirmation.

To pay a utility bill, the customer can have an SMS message alert set up so that he is prompted every time a payment is due. To make a payment, the customer would only have to reply to the SMS message and would then receive the IVR call for authentication.

PayMate can be used in retail stores as well. Here, the mobile number is provided to the cashier and the rest of the process works the same as above.

Enrolment: The process of enrolment has been delegated to the banks in this business model. PayMate has tied up with a few banks as partners. This means that PayMate is available only to customers of these partner banks. In total, there are six partner banks. The enrolment process varies from bank to bank. ABN

[24] All information, unless otherwise mentioned, from (www.paymate.co.in, 2008)

AMRO lets its customers enrol via internet or phone banking; new customers are given the choice of enrolling for PayMate when they are applying for their account/credit card. Cosmos and Corporation Bank on the other hand, let the customer enrol for PayMate via their ATMs.

The advantage of this kind of an enrolment process is that there has already been a certain level of authentication of the customer before-hand when opening the bank account or credit card. As far as the banks are concerned, they have already established the customer as a trusted counterparty. As banks are already involved in authenticating their customers, it is not a new process to them and enables each player to concentrate on their core competency.

Indian Railway Tickets

The Indian Railway Catering and Tourism Corporation (IRCTC) has teamed up with different players to offer enquiry and booking of railway tickets via the mobile device. The IRCTC has partnered with ngpay, the MNO Airtel and the ICICI bank to provide mobile ticketing to each of their respective customers.

Although there are 3 different partnerships, the method of booking the ticket is fairly similar. All of them are SMS-based. Although extensive research was undertaken, it is not quite clear if all three of these services are still offered or if only one of them have emerged to be Indian railway's choice of payment.

The IRCTC is one of the ngpay's merchants. So, to book railway tickets using ngpay, all the customer would have to do is choose IRCTC from the list of ngpay partners. The customer can then check railway time tables, check ticket availability and book his ticket (www.ngpay.com, 2008). To pay, the customer would use his card that is stored in ngpay. On successful booking, the customer is given a Passenger Name Record (PNR) number as confirmation. Ngpay also holds a booking history which the customer can access at all times. The ticket – referred to as an i-ticket – is sent to the customer by courier service.

In partnership with the IRCTC, the ICICI bank also offers mobile railway ticketing to its customers. For this, the customer needs to register with the bank for mobile banking and for their mShopping service (this step essentially involves creating a so-called mShop name which functionally works as the PIN for mobile transactions) and then with the IRCTC as well for their mobile ticket booking service (ICICI Bank, 2008).

To make a booking, the customer first sends an SMS message enquiry to the IRCTC who then reply with the availability status and the billing amount for the ticket. To confirm booking of the tickets, the customer would then send a return SMS message to authorize the payment. This message will also contain the mShop name. On successful booking, the amount is deducted from the customer's bank account with which he is registered and the customer is sent his PNR number via SMS messaging[25]. The ticket is then sent to the address with which the customer is registered at the IRCTC (ICICI Bank, 2008).

As can be seen, the mPayment scenario is India is still very young and is more SMS based. The fact that there are more people using mobile phones than the internet and the fact that it is not restricted to the upper income class, make it cover a wider audience of people. However, to reach the huge mobile population, the mPayment services would have to be simple to use, affordable and should also be made possible without the user having to hold a credit card as the Indian lower-income customer may not be in possession of a credit card.

4.1.4. Australia

Australia has a population of approximately 21 million as of 2008 (International Telecommunication Unit, 2008). The PSTN subscription rate is about 45% and the mobile penetration rate is 105%. Around 72% are internet users. Australia has

[25] There have been user reports stating that mobile booking with the IRCTC and ICICI is not always successful and that network issues have caused users to lose money due to the bank having sent the payment, however the IRCTC not having received it and thereby not issuing the ticket (http://www.amitbhawani.com/blog/indian-railways-online-ticket-booking-services/); this would seem highly unlikely as there would need to be stringent regulations in place ensuring a secure payment as with all sorts of digital payment systems.

had mPayment applications for many years now. Below, a few of the more recent mPayment applications used in Australia are described.

mHITs[26]

mHITs is an mCommerce platform that can be used to make P2P payments over the mobile device using SMS messages and was introduced in 2004 as a simple means to recharge prepaid mobile accounts via SMS messaging. Today, mHITs has expanded to be an mPayment application from which the user can make payments from one mobile phone to another and can also pay for purchases like electronic or mobile content, and micro-payment purchases (mHITs, 2008b).

How It Works: To transfer cash, the user sends an SMS message to the pre-specified number supplied by mHITs[27]. The SMS message contains the mobile number of the recipient, the value and an optional comment. The sender then receives an SMS message updating him on the balance in his account and the status of the transaction just made. The recipient also receives an SMS informing him of the payment made to him. mHITs also enables peer-to-peer (P2P) money transfers to mobile numbers that are not registered with mHITs; however, only the transfer between mHITs members is free of charge.

Using mHITs for purchases works in a similar fashion: the customer sends an SMS message to the mHITs number specifying the amount, a reference and the ID of the merchant who is supposed to receive the payment. The different types of payments are distinguished by keywords in the SMS message. For example, to make a P2P payment, the SMS message would be prefixed by the keyword **<pay>** while to make a payment to a merchant for goods purchased, the keyword **<buy>** would be used. Other keywords include **<balance>** to check the mHITs account balance and **<bank>** to transfer money to a bank account.

The advantage of mHITs is that it is pretty much device-independent. All it requires is a mobile device capable of sending SMS messages, which all mobile

[26] All information, unless otherwise mentioned, from (MHITs, 2008a)
[27] Pre-specified Number: 0428 696 448

phones can today. The only cost involved is the network charges of sending the SMS message.

Enrolment: Enrolment is done through the mHITs website, specifying the mobile number, personal details and email address. Before making a P2P or bank account transfer, the user has to top up his mHITs account with credit.

Players Involved: mHITs itself is the main active player in this mPayment scenario. As all the payment instructions are sent via SMS, the MNOs again only have a very small degree of participation. The other players would be the merchants who offer mHITs as a payment option.

Visa payWave/Telstra Contactless mPayment[28]

The Australian MNO Telstra along with the National Australian Bank (NAB) and Visa International offered contactless mPayments using Visa payWave to customers at Melbourne's Docklands. The 3 month trial ended in February 2009 and was considered a huge success.

How It Worked: Visa payWave is a good example of a mobile proximity payment application. Customers were required to download the NAB Visa credit card software onto their mobile device; this software stored their credit card details. To make a payment, the user waves his mobile phone in front of the merchant's POS reader. The data is read and transferred using NFC technology to the merchant's reader and the payment is processed like any other credit card payment. As such, there is no kind of authentication in the process: no signature or PIN is required. The status of the transaction can be read off the merchant's reader. Using this, customers can pay for low-value transactions that are under $35 Australian Dollars only.

Players Involved: As this was only a trial run, the players involved were Telstra, NAB and Visa International. There were 12 merchants involved and 200 users tested the application.

[28] All information, unless otherwise mentioned, from (Telstra, 2009)

Enrolment: For the trial run, there was no explicit enrolment process. NAB chose 200 of its customers to test the application.

Gauging the success of the trial, Telstra anticipate that there will be a consumer demand for contactless mPayments. As part of the trial,

- 95% of the participants said that there were likely or extremely likely to use the technology
- 78% of the participants found using contactless mPayments was better than using cash.

(Telstra, 2009) continue to say that even the merchants found it to be a quicker and more convenient payment option.

Visa payWave is already available in the form of a contactless card payment facility in many countries. Apart from Australia, Visa has conducted trial runs for the mobile version in Switzerland, Spain, France and the UK amongst others (Visa International, 2009). The UK trial called the "O2 Wallet" lasted six months between November 2007 and May 2008 involving 500 users. This trial included storing the Oyster card[29] in the wallet (Nokia, 2008).

4.2. Europe

When compared to Asia, the mPayment scenario in Europe is not that established. Europe tends to prefer the more conventional payment methodologies. (Gartner Inc., 2008) attributes this to the user's higher sensitivity to security as well as the good payment infrastructure available. Nonetheless, there are quite a few mPayment applications, a cross-section of which are illustrated below.

4.2.1. Germany

With a population of approximately 82 million, Germany has a mobile subscription percentage of around 130% (International Telecommunication Unit, 2008). Around 76% of the population are internet subscribers and 63% are PSTN

[29] The Oyster Card is a card-based transport ticketing system used in London, UK. See Appendix for more details.

subscribers. Although Germany has a saturated mobile penetration, mPayments have not made it very far in this country. This is largely because the German population does not see the necessity for a new payment option and they prefer the traditional payment systems (Hampe et al., 2003a). An example of a successful mPayment application in use in Germany is the "Get In" application – a mobile ticketing application used in the city of Hanau. Germany has also seen a venture of biometric payment, which is also explained below.

RMV Hanau HandyTicket (using NFC)[30]

The *Rhein-Main-Verkehrsverbund* (RMV), the public transport company of Hanau, Germany, introduced the mobile ticketing scheme "Get In" using NFC technology. The pilot programme was started in May 2005 with 160 users and partnered with the Hanauer Strassenbahn AG (HSB), Nokia and Philips. To use this, customers had to purchase the Nokia 3220 phone whose shell is equipped with an NFC chip.

The pilot ended in April 2006 and, due to its success, is now available to all customers of the RMV. Although initially it was known as Get In, the mobile ticketing feature has expanded to include more features like sorting timetable, older tickets and billing details and is now known as the RMV Hanau HandyTicket and is available using NFC technology.

How It Works: When boarding a bus, the customer goes to the NFC terminal and holds his mobile device in front of it; the required data is read and the customer is "checked-in" for the journey. When he leaves the bus, he has to hold his device against the terminal again to "check-out". Billing is done on a monthly basis and is debited from the customer's account. The total bill is calculated using the "best-price system" where the most economical price is calculated for the customer depending on usage.

Players Involved: The players involved in the HandyTicket scheme are the RMV, Nokia, Vodafone and T-Mobile. While RMV is the payment provider,

[30] Unless otherwise mentioned, all information taken from (RMV, 2008)

Nokia provides the NFC equipped mobile phones. Vodafone and T-Mobile are the MNOs that facilitate the HandyTicket to their customers.

Enrolment: To use the application, the customer has to first register online on the website of the RMV (www.rmvplus.de). Here, he enters his details like name, address, mobile number and email address. The user sets up an online account. After registering online, the customer receives an SMS stating that his registration has been successful and providing a link to download the required software. This installs the ticketing software that will be used to buy tickets, store them and that can be used to download the timetable.

Figure 11 – Hanau HandyTicket NFC Terminal in a Bus[31]

The Hanau HandyTicket is the perfect example of how an mPayment/mTicketing application fits the bill of added convenience. All the customer has to do is touch in and touch out his mobile device at the ConTag terminals as shown in Figure 11, and he is automatically billed for the ticket. Also, the hassle of choosing the right ticket is taken off the shoulders of the customer as the best price is calculated for him by the application. It rids the customer of the paper ticket that he has to carry

[31] Source: http://www.rmv.de/coremedia/generator/RMW/Kontakt/Presse/Bilderdownload/PM_BILD_HandyTicket_070424.html

on him. Security and authentication is provided by the mobile PIN. This system could be replaced by a biometric authentication system. The fact that there is a software in place that handles all the ticketing details makes it even easier as this software can be enhanced to include this feature.

HandyTicket - Deutsche Bahn[32]

The Deutsche Bahn (German Railways) offers mobile tickets for their rail network. Here, the ticket is sent to the customer in the form of Multimedia Messaging Service (MMS) message.

How It Works: To purchase a ticket, the customer accesses the site http://mobile.bahn.de set up for this purpose from his mobile device. Here, he enters his travel details, based on which a list of possible connections is retrieved. The customer then chooses his preferred connection and is prompted for his user name and password which are set up during enrolment. On successful authentication, the customer is given the choice of making a seating reservation. After confirming the travel details that have been entered the customer is asked to enter the mobile number to which the MMS ticket should be sent. By default, the number with which the customer registered himself is shown; however, any number can be specified, meaning that the purchaser of the ticket and the traveller need not be the same, which is an advantage. After selecting the mode of payment (credit card or direct debit), the customer finally confirms his booking. An MMS containing the ticket is sent to the specified mobile number and an email confirmation is sent to the registered email address. Payment is then processed as a normal card payment.

Enrolment: The customer has to first enrol/ register online before he starts using the application. This enrolment process is very minimalistic, requiring the user to set up a user name, password and provide his personal details like name and address.

[32] Unless otherwise mentioned, all information taken from (www.bahn.de, 2008)

For customers travelling with the Deutsche Bahn, the MMS ticket service is a very convenient method of purchasing tickets, considering the long queues at the railway POS and the lengthy procedure one has to go through at the ticket vending machines. Also, the customer does not have to incur any additional charges, except those incurred to connect to the internet. The Deutsche Bahn saves on ticket printing, avoids long queues at the ticket counters and provides a value-added service to its customers. A drawback that this system has is that customers who do not have mobile devices facilitating MMS cannot use it. However, the number of non-MMS enabled mobile devices is diminishing.

DigiPROOF

The first biometric payment system – digiPROOF – in Germany was introduced in the supermarket chain Edeka in the city of Rülzheim by IT-Werke[33]. DigiPROOF is a payment method where the customer verifies and authenticates himself using fingerprint verification.

Figure 12 – Customer paying at an Edeka Supermarket [34]

How It Works: The main advantage that digiPROOF has, is that is does not require any additional object: no card or mobile device. To make a payment, the customer places his finger on the fingerprint scanner as shown in Figure 12; on

[33] All information, unless otherwise mentioned, from www.it-werke.de
[34] Source – www.manager-magazin.de/unternehmen/it/0,2828,grossbild-446185-345932,00.html

successful authentication, the amount is debited from the customer's bank account. These details were recorded during enrolment.

Players Involved: The number of players involved with digiPROOF is minimal. It is offered by it-Werke, an IT solutions provider. The other players involved are the banks and the merchants that accept digiPROOF as a payment option. DigiPROOF started with Edeka, a supermarket chain in Germany. The list of merchants is slowly growing and includes supermarkets like Metro and Globus, Albert Heijn in the Netherlands, a food courts as well as in a school canteen in Germany.

Enrolment: To enrol, the customer has to produce his identification card, bank details and give his fingerprint. Apart from this, he also has to present his credit history document. Compared to enrolment for mPayment applications, the enrolment for digiPROOF is more meticulous as it does require the user to present his identification, and confirm his credit credibility.

4.2.2. Norway

Norway has a population of about 4.7 million. It has a mobile penetration rate of around 111% and a PSTN subscription rate of just around 40% and 88% of internet users (International Telecommunication Unit, 2008).

LUUP[35]

LUUP is a payment system that started in Norway in 2002 under the name Contopronto. LUUP is also an mPayment system that makes use of a digital wallet. What differentiates LUUP from many other mPayment applications is that it facilitates the transfer of P2P payments. A positive aspect of LUUP is that it is not MNO dependent; the customer only requires a mobile device, similar to Australia's mHITs.

How It works: To make a payment online, the customer chooses LUUP as the payment method, enters his mobile number or username and his PIN code. A

[35] All information, unless otherwise mentioned from www.luup.com

verification code is then sent to the mobile device of the customer, which he then enters online to complete the transaction. To make a person-to-person payment, the customer simply sends a text message stating the mobile number or username of the recipient as well as the amount to a preset LUUP shortcode number. LUUP will then credit the account of the recipient with the given amount. At the time of writing this thesis, LUUP only facilitates the purchase of mobile content like ringtones and games through the mobile device. Again, this utilizes the SMS facility to send a message to the mobile content provider who will contact LUUP to confirm the availability of sufficient funds.

When making a purchase, the payment amount is deducted from the option that is selected as the default payment option.

Enrolment: Enrolment takes place online (www.luup.com) where the customer enters his personal details. On successfully entering all the details, the customer is sent an SMS with a verification code which he enters online to complete registration. The LUUP wallet can be used online as an eWallet as well as on the mobile device as an mWallet. The customer can register his credit cards or debit card with his LUUP wallet or pay money into the wallet by transferring funds from the user's bank account.

Apart from Norway, LUUP is also available in the UK, Germany and Abu Dhabi. According to (Wray, 2006), LUUP had more than 10,000 customers each in the UK, Germany and Norway as of May, 2006. In 2009, LUUP partnered with Deutsche Bank to offer a cross border mPayment service (LUUP.com, 2009)

4.3. North America

A few applications from The United States and Canada are discussed here.

4.3.1. United States of America

The United States with a population of around 311 million people has a mobile penetration rate of approximately 87% as of 2008 (International Telecommunication Unit, 2008). Unlike Europe which is based on the Global System for Mobile Communications (GSM) network, the US mobile network is

covered by the Code Division Multiple Access (CDMA) as well as GSM. One of the differences between GSM and CDMA phones is that the CDMA does not use SIM cards. This becomes relevant if the chosen biometric template is supposed to be stored in the SIM card; while a CDMA user could use the BiMoP application by storing the data on the phone, the disadvantage is that the user becomes device-dependent. The user would not be able to simply switch SIMs from one mobile device to another.

Pay By Touch

Pay By Touch was a biometric payment application provided by Solidus network that started up in 2002 (McKinney, 2008) in the United States. Pay by Touch used fingerprint verification and allowed customers to pay for their supermarket shopping by merely authenticating themselves with their finger just like digiPROOF.

However, Pay by Touch filed for bankruptcy in December 2007 and shut down all operation in March 2008 (Payment News, 2008) although it had a 3.6 million customer base and was operational in approximately 3000 locations (McKinney, 2008). Many reasons have been cited for this ranging from the founder's reputation to the lack of consumer willingness to adopt biometrics as a means of securing their payment information.

An article written by (Carpenter, 2008), a former Pay by Touch employee, sums up the possible reasons as follow:

- *Consumer Adoption of Biometrics:* Although Pay by Touch did have several hundreds of transactions a month, there were still people hesitant to trust biometrics for reasons cited in Chapter 3. Although there were early adopters, the vast majority of consumers did not feel comfortable using biometrics on issues of privacy and still preferred conventional credit cards.

- *Economics of Biometrics:* Although prices have reduced over the years, biometric hardware is still an expensive investment, according to (Carpenter,

2008). For Pay by Touch, equipping and replacing the required hardware periodically at the participating grocery stores was an expensive affair; transaction costs had to be kept low as well. This meant that operational costs had to be kept low, but unfortunately didn't happen.

- *Level of Certainty in Authentication:* As explained in Chapter 3, the two important metrics involved with biometrics is the FAR and the FRR which are inversely proportional. One of the major difficulties with biometrics is finding the right threshold value during authentication to avoid false rejects and false accepts. However, the less the number of false accepts, the greater the number of false rejects. Pay by Touch concentrated on having a low false accept rate so as to avoid wrong accounts being debited. This meant that the false reject rate was high resulting in consumers losing confidence in the payment application.

How It Worked: Pay By Touch was basically a virtual wallet that not only stored payment details, but also identification data like the driving license number or other ID card numbers. It also held information pertaining to the different loyalty programmes that the customer takes part in. This virtual wallet was stored in a central server and the data accessed using the fingerprint of the user.

To pay for goods, the customer placed his finger on the reader at the POS and entered his search number as specified during enrolment. Using this search number could actually be considered as a disadvantage since it requires the user to remember an additional number needed to identify him. Once the search number is entered, the virtual wallet was accessed and the customer then selected the payment type from the virtual wallet. The rest of the payment was processed like any other normal card payment.

Enrolment: Enrolment took place in two stages – in the first stage the customer registered his personal details, his payment details and his driving license number or ID number. This could be done either online or directly with one of the Pay by Touch merchants. In the second stage, the customer had to enrol his fingerprint. This could be done during the customer's first purchase at one of the Pay by

Touch merchants. During enrolment, the customer also specifies a seven-digit search number, which will be used to access his wallet more easily. This search number would serve identification purposes and can be any number that the customer can easily remember.

Like digiPROOF, Pay By Touch was a payment system that used biometrics for authentication purposes. The search number in Pay By Touch could be replaced by the mobile phone number, thereby eliminating the requirement of an additional number. As the wallet would be saved on the phone in the case of mPayment, the authentication would also be carried out on the phone so as to access the mWallet. The data would then have to be transferred to the POS terminal.

MasterCard PayPass – "Tap N Go"[36]

Similar to Visa's payWave, MasterCard offers a contactless payment facility called PayPass. PayPass too, was initially introduced as a contactless card payment option where the user waved his card over the POS reader. MasterCard conducted a trial run in New York for the mobile phone option. Today, PayPass Tap& Go is available in the US, the UK, Australia, Canada, Japan, Korea, Malaysia, Philippines, Taiwan, Thailand and Turkey[37]. While no explicit information was found as to whether all these countries provided the mobile phone version of PayPass Tap & Go, the POS reader is capable of connecting with the contactless cards, NFC-enabled phones as well as NFC key fobs. Therefore, the availability of the mPayment version would depend on the banks and MNOs offering NFC-enabled mobile devices with the PayPass application.

The NYC Mobile Trial[38]: The NYC trial was conducted from January to April in 2007. It equipped the users with NFC-enabled Nokia trial phones to make payments at PayPass merchants. The trialists could also use the mobile PayPass to buy subway tickets on one subway line as well as download information from so-called smart posters. For this, the user had to tap his phone on posters which were labelled with the trial symbol; then, he could download content such as movie

[36] All information, unless otherwise mentioned, from (MasterCard International, 2008)
[37] www.paypass.com
[38] (MasterCard International, 2007)

trailers, wall papers and restaurant ratings amongst others. The trial was a joint venture between MasterCard, Citigroup, Cingular and Nokia. Nokia issued the NFC-enabled phones, Cingular is the MNO and Citi is the issuing bank. As a part of the trial run, selected Citi credit MasterCard customers were given NFC-enabled Nokia phones which contained their credit card details. Since this was only a trial, there was no explicit enrolment procedure. A similar trial was conducted in Ontario, Canada for 4 months which ended in April 2009.

How It Works: When making a purchase, the customer activates PayPass on his mobile device and then taps the phone on the PayPass reader. When the transaction is completed, the reader beeps and flashes a light. The rest of the transaction – clearing, settlement and management – would be carried out in the same fashion as a regular credit card transaction.

Enrolment: Enrolling for PayPass would be carried out through any of the issuing bank players. As mentioned above, it is not clear how PayPass Tap N Go with mobile phones is in use in the market apart from the trial runs.

An interesting innovation that MasterCard has recently introduced is the Blaze Mobile MasterCard PayPass mobile payment sticker (MasterCard International, 2009) for Tap N Go payments. This sticker is equipped with the NFC unit that needs to be tapped to make payments. Unlike regular PayPass payment devices, the sticker is not connected to a credit card, but is tied to a prepaid account with MetaBank – the issuing bank player. The main advantage that the sticker brings with it is that it makes the mobile PayPass Tap N Go available to customers who do not possess NFC-enabled phones. The sticker will also be offered to the MasterCard Blink customers of the Chase bank starting Spring 2009 up to October 2010 in a trial version[39] . Blink is the same as PayPass.

4.3.2. Canada

Canada has a population of about 33 million: around 65% of these are mobile subscribers, 55% PSTN subscribers and 75% are internet users (International

[39] www.chasemobiletag.com

Telecommunication Unit, 2008). As mentioned above, MasterCard is conducting a trial run of PayPass in Canada until October 2010. Another mPayment application is described below.

RBC MOBEX[40]

Mobex is an mPayment service offered by the Royal Bank of Canada (http://rbcmobex.com). The trial run for the service completed in early 2009; however, it is not clear for how long the trial period ran. During the trial run, Mobex was available to RBC staff, their family and friends. The primary function of Mobex is to send and receive money. Users of any network could participate: the only requirement was to have a bank account and a mobile device.

How It Works: Mobex works using SMS messaging. The user requires a Mobex account which is set up during enrolment. This Mobex account essentially works like an eWallet that is accessible via the mobile phone or through the Mobex web portal. The user loads funds to this Mobex account from his bank account or his Visa or MasterCard credit cards, which were set up during the enrolment process. This is done by sending an SMS message to a pre-defined number with the keyword **ADD** or **CASHIN** followed by the amount. There is a daily load limit of $100 and a monthly limit of $500. Once the user has transferred the funds to his Mobex account he is ready to send money; while the recipient does not need to be a Mobex account holder at the time of sending, he cannot access the money till he has registered and opened a Mobex account. To perform the send, the user sends an SMS message with the keywords **SEND** or **PAY** followed by the recipient mobile number and amount in any order. The amount is then deducted from the Mobex account. The user can also check his account balance by using any of the keywords: **BAL, BALANCE, CHECK BALANCE** or **CHECK BAL**.Another functionality that Mobex provides is the ability to request money from another Mobex user. Again, this is done by sending an SMS message to the pre-defined number with the keyword **GET** or **REQUEST** followed by the amount and mobile number in any order. All these operations are accessible through the Mobex web portal as well. The transaction history can also be viewed.

[40] All information, unless otherwise mentioned, from (http://rbcmobex.com, 2009)

Players Involved: Unlike most other mPayment applications, there seem to be no other active players associated with RBC Mobex except for the RBC. Since the user transfers funds from his bank account or credit cards like he would pay for any other transaction, other banks cannot be seen as mPayment players. Similarly, from the MNO perspective, the MNOs only transfer the SMS message as they would do with any other SMS message between two phones. Hence the only active player involved with Mobex is the RBC.

Enrolment: The enrolment process takes place online over the RBC Mobex web portal. It can be split into four parts:

1. *Proving Personal Data*
2. *Mobile Phone Number Verification*
3. *ID Verification*
4. *Account Activation*

1. *Providing Personal Data:* The first step of the enrolment process is for the user to provide his personal details like name, address, occupation, phone numbers and email address. Additionally, the user sets his 4-digit PIN that he will be using to authenticate himself during transactions. The user also has to set up a separate password that he will be using when accessing the RBC Mobex web portal and has to set up a verification question that will be used to authenticate the user should he call the RBC Mobex customer service. The user also accepts the terms and conditions in this step.

2. *Mobile Phone Number Verification:* Once the user has entered his data, confirmed the details, an SMS message is sent to his mobile device containing a one-time passcode. He has to enter this passcode in the web portal thereby verifying his mobile number.

3. *ID Verification:* Unlike many other mPayment applications, RBC Mobex requires customers to verify their identification. The ID verification is also done online on the web portal, however it is not clear how this is performed. In case the online verification process cannot be completed, the user has the

possibility to complete the verification at any RBC bank branch. For this, he needs to present two forms of identification; atleast one needs to be a photo ID and atleast one needs to be a government-issued document.

4. *Account Activation:* The final step in the enrolment process is the account activation. In this step, the user provides his bank details and/or credit card details from which he would like his funds to be drawn. Again, this is performed through the Mobex web portal.

The trial run for RBC Mobex completed in January 2009 and users were able to still use the service till the end of February 2009. The RBC Mobex accounts were completed closed in March 2009. It is not clear how successful the trial was or if the service will be launched to the public.

5. Using Biometrics in an mPayment Scenario

This chapter will analyze how fingerprint verification or speaker verification could be implemented in mPayments. The factors that need to be considered, the enrolment process as well as establishing the appropriate player to carry out enrolment will be discussed.

5.1. The Issue of Enrolment

Authentication in any form starts with the enrolment process. In the generic sense, the enrolment process deals with capturing personal data and features of the enrolling person, such that these help to authenticate and verify the person at a later stage. Biometric enrolment deals with capturing the biometric features of the person, processing them and converting them into a biometric template that is then used for the authentication process.

In any payment system, or in any secure system for that matter, there is always an enrolment process. It could be something as simple as capturing the name, user name and password in creating an online email account. An initial enrolment process captures valid information that helps establish the identity of the customer. Even when a customer applies for a credit card the issuing company takes the customer through an enrolment process which also includes performing a credit check of the customer's financial history.

In biometrics, enrolment can be a difficult process not just because of the equipment, time and resources required, but also because each person provides their biometrics differently. While some people may be able to work perfectly with some sensors, others may find it difficult to use these at all. Similarly, while some customers may be enrolled easily into a biometric system, others may find it more difficult. Apart from this, the features of some people may be easily forged. These factors would need to be considered when enrolling a person. For instance, should the threshold value be set higher for some and lower for others who find it

difficult to use a biometric system? The performance variability of different users is described by (Doddington et al., 1998).

5.1.1. Performance Variability - Doddington's "Zoo"[41]

As mentioned in Chapter 3, some biometrics have certain behavioural aspects attributed to them. This means that each time the biometric is captured, it can vary slightly from the template or the previous capture. There is a behavioural aspect involved even with the physiological biometrics – the way the user places his finger on the reader, the pressure applied - it all can change the print captured and hence affects the level of recognizability. This level of recognizability varies from person to person. (Doddington et al., 1998) use the animal world to categorize users, based on their level of recognizability, into 4 separate classes; the animals used are goats, sheep, wolves and lambs. This classification is based on the performance variability of each individual (Doddington et al., 1998). Although this concept was introduced in context with speaker recognition, it could well be extended to all biometric authentication methods, however not as expansive as with speaker recognition. For example, while the concept of sheep and goats can be considered universal with all biometrics, the probability or rather the possibility of forging biometrics like retinal scans is close to zero. Traditionally, the population was classified into *"sheep"* and *"goat";* this was extended to include the wolves and lambs.

Sheep: Doddington names those individuals who take a natural affinity to the system as sheep. The sheep are individuals who perform well with the biometric system. Most individuals fall under this category. Based on this, sheep should be fairly easy to enrol as the performance variability is comparatively minimal.

Goats: Those individuals whose biometric sample is difficult to recognize are labelled as goats. This results in individuals being falsely rejected and therefore increases the FRR affecting the overall performance of the biometric system. Given the difficulty in recognizing goats, enrolment for these individuals should be carried out very carefully and the sample biometric should be captured multiple

[41] The concept of the "Zoo" taken from (Doddington et al., 1998)

times to ensure a good template. Goats should be identified early on in the enrolment stage. Care should be taken to ensure that the template and the threshold value are set such that the individual is easily recognized. However, making an individual easily recognizable also means that his template is more susceptible to fraud. A balanced value should be considered to avoid fraud while at the same time ensuring that the correct person is authenticated.

Lambs: The lambs are those individuals whose biometric can easily be forged. There are possibly more lambs when using behavioural biometric authentication techniques, like signature verification or speaker recognition, as when compared to using physiological biometrics. This is because the behavioural aspects of humans, although underlined by certain physiological characteristics, are easier to imitate. Sometimes an impostor can use his own biometric sample to claim the identity of an existing enrolled person. This is known as *zero-effort forgery* (Bolle et al., 2004). An example of zero effort forgery would be forging a signature.

Since they are easy to imitate, lambs enrolled in a system affect the system performance by causing a large number of false accepts thereby increasing the FAR.

Wolves: Wolves are those individuals that are good at imitating others, usually the lambs. Unlike lambs, sheep or goats who are all enrolled users, wolves are not enrolled users of the biometric system. They are intruders who cause a large number of false accepts. Although lambs cause false accepts as well, the underlying mechanism between the two is different. While the lambs passively cause false accepts, wolves cause them actively (Bolle et al., 2004).

Chameleon: Chameleons are individuals who can be easily imitated and who are good at imitating others (Bolle et al., 2004, p. 163), causing both passive and active false accepts.

When enrolling a person, it is important to identify which category the user would fall under. Enrolling lambs would require a high threshold being set and educating the user to correctly use the system so that he is not falsely rejected. Similarly,

when enrolling a goat, multiple samples of the reference template would need to be collected and it might be worth setting a low threshold value.

5.1.2. The Enrolment Process

Enrolment is of great significance as it can make or break the credibility of authentication. All subsequent verification instances are conducted against the template generated during enrolment (Nanavati et al., 2002). Erroneous enrolment would eventually result in erroneous verification. It is vital therefore to establish the correct identity of the person. Especially in the case of mPayment, where it is the financial details of the customer that requires protection, extreme attention is called for to ensure that the correct identification of the person is established and the right information captured.

Ideally, the enrolment process has to be carried out in the same fashion for all individuals. The physical enrolment process should have been documented in advance (Ashbourn, 2004) and checked for flaws and loopholes. There are many aspects that need to be considered before the actual enrolment process can begin; an adequate threshold value needs to be calculated, alternate arrangements need to be available in the case where an individual cannot enrol. It needs to be decided if an individual threshold value be set for each individual or if a common threshold value is used taking into account the costs involved. All these are questions that need to be answered prior to enrolment taking place. After enrolling an identity, the template should be checked for its usability (Ashbourn, 2004). It should also be checked if the user knows how to use the system and if he is able to verify himself properly. These steps are all discussed individually below.

1. Setting the stage – Crucial Aspects prior to Enrolment

Prior to the actual capture of a person's biometric data, the identity of the individual has to be verified. Establishing the true identity of the person is perhaps the most significant part of the enrolment process. If a person is enrolled as somebody he isn't, he will each time be verified as somebody he isn't and can thereby assume a false identity. For example, if person 𝔸 claims to be person 𝔹 and is enrolled as 𝔹 without further investigation, 𝔸 will always be identified and

verified as B. Therefore, biometric authentication does not really verify who you are, but verifies who you are enrolled as. This makes enrolment a significant process so crucial and makes the established identity of a person prior to enrolment crucial to the proper functioning of biometric authentication systems. *"A user who enrols in a biometric system under a false identity will continue to have false identity verified with every successful biometric match"* (Nanavati et al., 2002, p. 11).

Establishing the true identity of the person to be enrolled bears utmost importance and is the first step in the enrolment process. The identity of a person can best be verified by means of adequate documentary evidence like passports, birth certificates, driving license and other certificates. (Bolle et al., 2004) refer to these documents as "seed documents". The information within these seed documents are referred to as the "ground truth". The risk of being provided with forged documents can be minimized by requesting the user to present multiple documents. Although we still run the risk of being provided with a set of forged documents, the probability is much lower since forging several seed documents is much harder (Ashbourn, 2004). It should also be insisted upon that multiple documents be provided and enrolment should only take place if all required seed documents are in place and the identity of the person could be securely established. In case of doubt with regard to the authenticity of the documents or if the seed documents do not provide sufficient authentication, the person should not be allowed to enrol. Ensuring this would avoid problems at a later stage. Half the job is done if the person to be enrolled has been verified to be trustworthy and consequently result in a robust system.

After the identity of the subject has been established, the capturing of the subject's biometric data takes place. Important factors that play a role in the capturing process are the environment in which the enrolment is being done, the hardware used, the software used, the personnel supervising the enrolment process and, not to be forgotten, the comfort level of the user. The more comfortable the user is, the better the outcome of the enrolment process will be.

The user should be given a good briefing with regard to how the enrolment process is to take place and how the process functions. Ideally, he should be informed well in advance before the enrolment day and should be briefed again, just before being enrolled. It is essential that the users have a keen understanding of the enrolment process, the technologies and policies in use (Bolle et al., 2004). This helps the user understand the system better and puts him at ease. Once the user knows how the procedure is carried out, a trial run of the enrolment process should be carried out to make the user comfortable with the system (Ashbourn, 2004). This also gives the user a chance to see how enrolment takes place and, to some extent, get familiar with the system.

The role of the workforce supervising the enrolment process should not be underestimated. They need to ensure that the procedure is carried out correctly, that the user is put at ease and that at the end a quality biometric sample is extracted. They need to take care that the user places his finger correctly on the scanner, speaks in the right tone and volume, or keeps his face in the right position for the enrolment of the fingerprint, voice or face, respectively. This can be made certain by training the staff adequately and regularly (Ashbourn, 2004).

2. Capturing Biometric Data

The next step is the capturing of the biometric data. A single run-through is not enough to form the biometric template. In order to extract the relevant features, the user will have to present his biometric a few times. The number of times a biometric has to be enrolled to create a single template varies from device to device and from technology to technology. (Nanavati et al., 2002) say that in the case of fingerprint scanners between one and six high quality presentations of a single fingerprint may be required for a single template. Fingerprint reading may also require that two fingers be enrolled, making it a total of up to twelve presentations. In the case of speaker recognition, a voice recording of around 30 to 40 seconds might be necessary to create a good voiceprint template. Obtaining a voiceprint is a more difficult process than obtaining the reference template for fingerprints. "*The only common element of these varied enrolment processes is the result: A user's information is eventually stored in some type of database or file for future comparisons*." (Nanavati et al., 2002, p. 33)

The user's presentation of his biometric data is essential to long-term performance (Nanavati et al., 2002). The way he presents his data during enrolment decides the way his live presentation is processed. Even if the biometric data is the same, the manner in which the user presents his biometric can lead to rejection (Nanavati et al., 2002) if he does it differently each time or unlike his presentation during enrolment.

Placing the finger at a different angle, purposely speaking in a different volume/ pitch can all affect the matching process and can result in *false non-matching* taking place. Speaker verification, being a behavioural biometric is more prone to changes in user presentation and special care need to be taken with this regard.

Perhaps the easiest biometric to enrol is the fingerprint. All the user has to do is place his finger on the reader. The angle, pressure used and maybe even the cleanliness of the finger are the decisive factors in this case. Hindrances could also come in the form of cuts or nicks during enrolment or during the live application. In such a case, where the user is injured on his "enrolment fingers", it might be a good idea to postpone the enrolment session till the wound has healed. There is also the risk of the user finding the whole process too tedious; and if the end-product – mPayment in this case – does not provide him with sufficient value-add, he may decide against it. One of the disadvantages of enrolment is that it requires a lot of user cooperation and user time. The end-consumer of the day is a "slothful" one who requires a lot of persuasion and who needs to see a tremendous increased benefit to change when he is actually quite happy with what he has at the moment. Given the situation today, where customers are quite content and satisfied with existing payment methodologies, this tedious enrolment procedure could have quite a negative impression on the user and would be something that he is not willing to do.

3. Compare Biometric Data to Existing Data

Errors in this initial stage lead to fake and/or duplicate identities being created. Note that there is a difference between a fake and duplicate identity. A fake identity is created when a person takes on a fictitious identity and enrols as such (Bolle et al., 2004). Enrolling with a non-existent identity can take place with the

help of forged documents or by using legitimate documents that have unknowingly been issued by an authority where the person was enrolled earlier. This means that the person/subject had already been leading a false existence with the given documents. While forged documents can be tracked (to understand that they are forged), it is difficult to break through the fraudulence of a person using legitimate documents since we trust in the authority who issued those documents. Such a case can have severe consequences, since with each instance of enrolment at a governing/ trust authority, the false identity of the person is strengthened more and more.

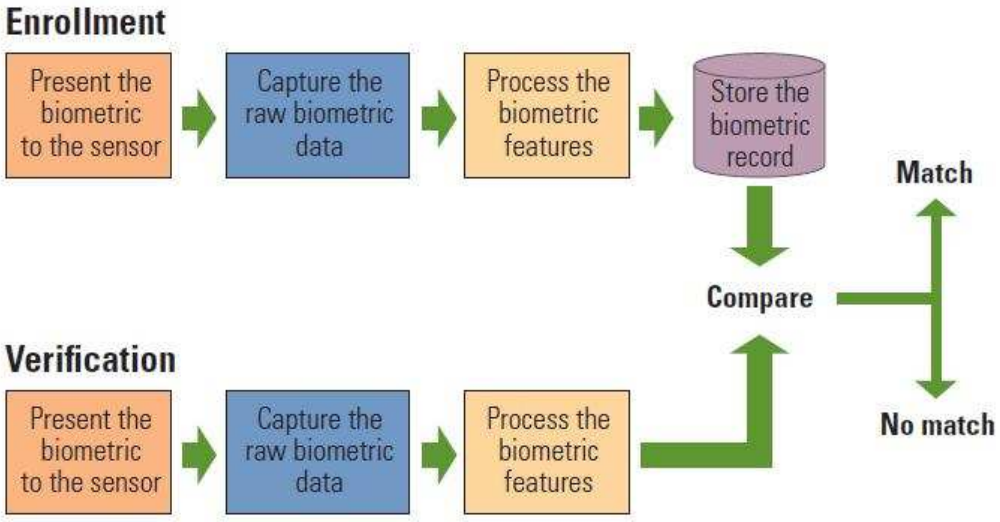


Figure 13 – Verifying the biometric data of a user (Tilton, 2006)

Duplicate identities are caused when a person falsely enrols with an existent identity or in other words, with the identity of a third person – a stolen identity. When enrolling a person, it is therefore necessary to check the existing enrolled entries in the database so as to avoid duplicate entries. Not only do we have to search for the same name entries, but we will also have to search for previously enrolled biometric data. These are measures that could reduce enrolment fraud, but which at the same time, cause tremendous overhead costs. Given the above, "*a biometric authentication system is only as secure as its enrolment subsystem*" (Bolle et al., 2004, p. 158).

To avoid/ reduce a case of multiple identities, every individual should be enrolled using the same finger, by the same software and possibly even with the same

hardware. A copy of the reference template should ideally be stored centrally. In the case of mPayment, storage of the template would preferably be in the mobile phone; however, maintaining a central copy would serve as a back up and could avoid the need for re-enrolment in situations like the loss of the mobile device or hardware failure of the mobile device. In such a situation, the whole enrolment process need not be repeated. You would only have to confirm if the person is authentic (which can be done by getting a fresh biometric sample from him and validating it against the back-up template).

4. Determining the Threshold Value

In biometrics, the enrolled template and the live one are rarely identical. Biometrics operate on the degree of similarity between the two templates. The more similar the two templates, the more likely they are to be from the same person. This degree of similarity is also known as the likelihood ratio (Bimbot et al., 2004) or the matching score (Nanavati et al., 2002) (Rila, 2002). Since in most literature, the term matching score is used, this thesis will use this term as well. The matching score/likelihood ratio is defined as "*the ratio between the probability that the person is genuine to the probability that the person is not the genuine identity*" (Bimbot et al., 2004). It is represented as:

$$P(Y \text{ from person})/P(Y \text{ not from person}) > \Theta$$

The verification process compares the live template and the enrolled template and produces the matching score. This value is then compared to the threshold value. The threshold value is a pre-determined value that is used as the decision factor in verification. If the likelihood ratio is above the threshold value, then the match is positive and if it is below the threshold value, it is a mismatch.

Hence, the threshold value can be defined as *"an empirically determined value such that all match scores greater than or equal to this value are considered positive matches for a given system."* (Woodward et al., 2003, p. 187)

Setting the threshold value is a difficult task. A high threshold ensures impostor acceptance is really low thereby reducing the FAR; however, this would also

mean that the number of false rejections increases and therefore would result in an increased FRR. Conversely, a low threshold value would reduce the FRR, but result in an increased FAR (Bimbot et al., 2004; Nanavati et al., 2002; Woodward et al., 2003).

When it comes to mPayment, the first thought would be to set a high threshold value since the underlying entity being protected is money. However, a high threshold could result in a huge population of dissatisfied customers in case of false rejections. This in turn may result in users not taking on the mPayment application as they would conceive it to "not work".

Finding a balance between the FAR and FRR and using an adequate threshold is an important part of the enrolment process. Given that biometric mPayment is meant to be a value-added customer application, a high FRR is not feasible. If mPayment is used mainly as a means to secure micro-payments, then it might be worth considering keeping a low FRR and risking a higher FAR since the potential loss can be controlled given that there is a cap on the payment value. Obviously, the resultant losses would be the responsibility of the providing players rather than the customer.

Another factor that needs to be considered when choosing the threshold is if a single constant threshold is used for all customers or if the threshold is set separately for each customer. Given the different types of users in Doddington's zoo model, a single threshold value for the biometric system would not be feasible since different individuals have different levels of susceptibility to false acceptance and false rejection. It would be more sensible to have a personal threshold value for each customer which is adapted to the way the user presents his biometric, whether he is a lamb, sheep or goat. Such a threshold value that is set for each person is known as a user-dependent threshold value (Bimbot et al., 2004).

A number of trial verification runs would have to be conducted to obtain the right threshold. Once the biometric sample has been captured and database verification has been carried out, a test run needs to be carried out. This test run aids to assess

the appropriate threshold value for the user. To start with, there would need to be a standard threshold value that can be adjusted depending on the test run. The test run would need to be carried out as often as required till a series of positive returns are obtained.

In their paper on speaker verification, (Bimbot et al., 2004) describe a system where two thresholds are used instead of one – an upper threshold and a lower threshold. A match score higher than the upper threshold would be considered a match and one below the lower threshold would be considered a mismatch. A match score that lies between the two threshold values would be considered "inconclusive". (Bimbot et al., 2004) further mention that in the case of an inconclusive match, the individual could resort to a secondary verification process like using a password or a different biometric. Such a setup would reduce both the FAR and FRR, but defeats the purpose of using biometrics with mPayments if the user has to remember a password.

To summarize, ideally there needs to be a standard threshold value that is used as the starting point. When enrolling the user, a number of test runs would need to be carried out to identify the ideal threshold value for the user. The standard threshold is adjusted to this level.

5. Authentication/Verification Rehearsal

After successfully enrolling the person, a test run of the verification process should be carried out (Ashbourn, 2004). This serves to get the subject accustomed to the application and also to check if the enrolment was successful. Immediately carrying out a live transaction would help in identifying potential "goats". In case a re-enrolment is required, it can be done straight away. In many cases, it may happen that the user cannot enrol at all. Such a situation is known as "Failure-to-enrol" and is expressed as the Failure-to enrol rate. For such situations, adequate back-up verification processes should be kept ready. A possibility would be to let the customer fall back to the password variant.

The verification rehearsal also aids in assessing the transaction time required. The transaction time is the *"theoretical time taken to match the live template against a*

reference sample" (Ashbourn, 2004, p. 10). For the success of mPayment, it is crucial that the transaction time be kept as low as possible. This is because the customer would not like to wait for more than, say 10 seconds, at the counter for his payment to get processed. In a biometric mPayment transaction, the transaction time comprises the time taken for the biometric authentication process and the time taken for the payment procedure to be carried out. The biometric authentication or verification process is depicted in Figure 13: the stored template details are compared to the live template and a match/no-match decision is made.

The biometric transaction time should ideally not take more than a few seconds. The verification rehearsal helps in assessing the transaction time for each individual subject as well as in assessing the average transaction time for all subjects.

During this test run, the users can also be trained to replicate the enrolment process. Some users may not be cognizant of the manner in which they enrolled, and may have to be guided a few times before they really understand how they can use the system effectively (Nanavati et al., 2002).

5.2. Factors affecting "Biometric" mPayment Systems

Implementing a system that has two new components to it brings with it a lot of factors that need to be taken into consideration:

- Technology: encompasses the kind of hardware, software and the data flow
- Economic factors: the cost-effectiveness of the application to all parties involved – customer, merchant and provider
- Human factors/Customer Acceptance: User psychology, ease of use of new system, user acceptance.

All these factors play a decisive role in the success of an mPayment system. This section will summarize the important factors that influence biometric mPayment systems. These factors would need to be considered when designing the business model for an mPayment system using biometrics. Additional detail has been given to customer acceptance as this is considered to be the most pertinent factor when it comes to the success of biometric and/or mPayment applications (Ashbourn, 2004; Zmijewska et al., 2004).

5.2.1. Technical Factors

For a combination of two differing technologies to work, there are a few technical factors that would need to be addressed before implementing a new system. For a biometric mPayment application, it would need to be decided, on a higher level, what hardware and software will be used, data storage, where the actual authentication will take place and so on. On a more detailed level, the type of interface between the biometric application, the mobile device and the mPayment application would also need to be laid out. For the scope of this thesis, we will only analyze the technical factors on a higher level. These factors are:

(a) Performance
(b) Transaction Time
(c) Template Storage
(d) Verification Process
(e) Interoperability

(a) Performance: The performance of the biometric mPayment application as a whole contributes to user perception and acceptance of the application. When we speak about performance, we refer to the technical performance of the application measured in terms of the quality of authentication as laid out by the performance metrics explained in Chapter 3, mainly the FAR and the FRR. Therefore, the threshold value indirectly affects performance. The FAR and FRR should be kept as low as possible.

Should there arise a scenario where a genuine user cannot be enrolled or authenticated using his fingerprint, there needs to be a fall-back authentication

manoeuvre that can be used instead (Ashbourn, 2004). Speaker verification or a PIN could be used as an alternative. Using a PIN protection method however would defeat the whole purpose and value-add that biometrics provide. Another back-up method would be to use a set of security questions to authenticate the user should the biometric method fail.

(b) Transaction Time: Apart from technical performance, the transaction time would also need to be considered as a performance factor. In a biometric mPayment application, the total transaction time would be the time taken for the entire transaction to be completed; this includes the time taken for the actual verification process as well as the time taken for the transaction to be authorized. This total transaction time is dependent on:

- Where the reference template is stored
- Where the biometric verification process takes place
- Speed of data transfer to the POS terminal (if applicable)
- Time taken for the transaction to be authorized.

The verification of the user and the time required for a transaction to be authorized are common to other generic non-cash payment methods such as credit or debit cards. As the mPayment application would ideally be built upon the existing infrastructure of such payments, the payment transaction time shall not be discussed in detail; the difference between them would be minimal. In a card payment, the customer would have to wait for the transaction to be authorized by the merchant bank and would also have to authenticate himself using the PIN or signature verification. At present such a transaction would only take about 30 seconds (Zmijewska et al., 2004). The biometric mPayment application should be at least on par with this time.

In a normal card transaction, once the transaction amount is authorized, the user verifies himself by signature verification. Alternately, the user enters his PIN number when requested to do so and is then verified. The biometric verification process would have to match this time taken to verify the user using the PIN method. The biometric verification process would prompt the user to give his

biometric sample and would then compare it to the reference template and provide a result.

Two factors would affect the speed of this verification process:

- Where the reference template is stored
- Where the verification process takes place

(c) Template Storage: Once the user provides the biometric sample, the reference template would have to be accessed for comparison. This reference template could be stored either remotely in a central database or locally on the mobile device. If the template were stored in a central database, this would result in additional network overhead; network protocols would have to be put in place and there would also be the danger of manipulating the data during the transfer (Ashbourn, 2004)[42]. This would also add on to the time taken for the verification process. Therefore in terms of improved transaction time, the better option would be to store the reference template on the mobile device. From a user perspective, this obviously gives rise to the question of how secure the reference template would be in the mobile device especially in the case of theft. The reference template in fingerprint verification is reduced to a set of points from which the actual fingerprint cannot be re-created. This would eliminate to a great extent that the reference template is tampered with and therefore render the reference template useless on its own. Of much more danger is the situation where someone would be in a position to replace the reference template with his own. The actual storage of the template should be secured the same way that the device/SIM PIN is stored, meaning that the template would be stored on the SIM card, rather than the phone. The additional advantage of this is that should the user change only mobile phones, he wouldn't have to reinstate the template as would be the case if it were stored in the phone.

[42] (Ashbourn, 2004) lists a possible set of five different verification processes and discusses which scheme would be best. While these schemes were referred to for this thesis, they will not be discussed in detail as they are of a more generic nature.

(d) Verification Process: The transaction time can also be affected by where the actual verification process takes place. Again, this can happen locally within the mobile device or the data can be transferred to a central server. If done centrally, the issue of transferring the data again comes into play, which gives room for data manipulation during transfer and increases transaction time. Also, since the template is stored on the SIM card of the mobile device, the best place to carry out the verification process would be the mobile device, reducing network overhead and associated costs, and ensuring a more secure application as well as maintaining a low transaction time. In mPayments, the transaction data will be transferred anyway to a remote server; the live template could be transferred with this data and the verification process could be carried out remotely. Although this is a viable option (without increasing costs since a data transfer and required infrastructure is already in place), it still leaves the securing of the mWallet open. Also, as the eventual aim is to provide an ubiquitous mPayment application that can hold cash and other cards as well, there doesn't always need to be a data transfer. At a vending machine, the user might just want to access the stored cash from his mWallet; this would not necessarily involve the transfer of data. Therefore, considering security, non-repudiation, speed of the transaction as well as ensuring an ubiquitous scenario, it would be best to store the reference template in the mobile phone and carry out the verification process in there as well. For additional verification, especially if the transaction amount is bigger, it could be contemplated sending the live template along with the payment data to the remote server for a further level of security.

To carry out a payment transaction, the payment data – the card/account number for instance – would have to be transferred from the mobile device to the POS terminal. Considering that all other processing takes place within the mobile device and the technology available and used in present day mPayment applications, this transfer is possibly best done using NFC technology from the mobile device to the POS terminal as is done in MasterCard PayPass explained in Chapter 4. Again this transfer should not take more than a couple of seconds so as not to add on to the total transaction time.

(e) Interoperability: Another technical factor is the "*interoperability across disparate systems"* (Ashbourn, 2004, p. 18). What Ashbourn is referring to is that many different systems will be used in a biometric application – for enrolment and for authentication at different times. The equipment/capture device used in all these situations should be in a position to produce the same set of results. In other words, the quality of the biometric sample or even the reference template should not be impinged upon by differing hardware.

Extending this idea to a biometric mPayment application, you not only have the problem with the variation between capture devices, but also have the problem of the way these capture devices interact with the mobile device. The mobile market today comprises a variety of different device models from different manufacturers; all of these need to be equipped with mWallets and need to be able to interact with the biometric capture device as well as the biometric verification software in the same manner. Also, different device manufacturers would use different biometric capture devices; these in turn could differ from the capture devices used during enrolment. Although it is possible to achieve the same result with equipment from different manufacturers, there is no guarantee. To overcome this problem, a set of standards should be in place for biometric mPayment applications. This not only has the advantage that it reduces varying performances due to hardware, but also lays the basis for an ubiquitous mPayment application using biometrics.

An option would be to use the customer's mobile device for the enrolment process. Since eventually almost all activity will be taking place within the mobile device, it might be sensible to perform the enrolment of the reference template using the device itself by connecting it to the centralized database where a copy of the reference template would be stored. This would minimize the difference in the template and the sample and would also mean a reduction in equipment costs used for enrolment. Furthermore, by enrolling himself using the mobile device, the user also gets accustomed to using the biometric capture device on his mobile device rather than an external one. It also ensures that the template quality will be the same as the same hardware is used.

In short, the technical factors not only influence the performance of the system, but also influence the business model of the BiMoP application. For instance, the location where the reference template is stored affects where the verification process is carried out and indirectly influences the transaction time as well as potentially influences the decision as to who carries out enrolment. Decisions have to be made with regard to the template storage and where verification is carried out. For a BiMoP system, the best option is to:

- Store the reference template on the SIM card of the mobile device.
- Carry out authentication on the mobile device
- Set individual thresholds for each customer
- Enrolment to be done using customer mobile device

5.2.2. Economic Factors

The payment methods available today are almost free of charge to the end-user barring the minimal annual fee that credit card companies charge. Given this, the mPayment application needs to be equally cost-effective to the end-user so that it remains competitive.

Building the biometric mPayment application as much as possible over existing infrastructure would reduce costs tremendously. This way, no new communication channels need to be added on, the requirement for extra hardware is kept to a minimum and additionally, the staff at the POS terminal need not be trained to use new equipment. As mentioned, it would be easiest to store payment details in the mobile wallet of the mobile device and to secure this using fingerprint verification. The data would then be transferred to the POS using infra-red/NFC technology. The rest of the payment process would now be carried out like any other card transaction. Utilizing the existing payment equipment and adding on the biometric reader and the required software to the mobile device would limits the costs involved. As mentioned in Chapter 3, there are already a couple of mobile devices with fingerprint readers on them

Along with the benefit of reducing the probability of template differences, using the fingerprint reader in the mobile device brings with it the hidden advantage of saving costs. This is because the player need not invest in new hardware to carry out enrolment.

5.2.3. Human Factors

There are a number of human factors as (Ashbourn, 2004) refers to them, that could affect a biometric mPayment application. To develop a system that is accepted by the masses, the system has to conform to their needs. Many mPayment applications have evolved over the years which have been technically sound, economic as well as secure; yet, a number of these applications failed to succeed in the market. The application's inability to attract a critical mass of users or in other words, **the lack of user acceptance** has been the main problem (Mallat, 2006). Similarly, fingerprint technology today is technically sound as well and relatively economical. However, the user perception of the use of biometrics hinder it from being used in mainstream applications for authentication. Similarly, although speaking is something that comes natural to the user, authenticating oneself using speaker verification in front of other customers at a POS terminal would be uncomfortable and the user might feel his privacy is invaded.

Below is a list of the human factors that affect customer acceptance:

(a) User Psychology
(b) Individual Characteristics
(c) Usability
(d) Privacy

The first 3 factors have been referenced from (Ashbourn, 2004). However, these have been applied to mPayments as well by the author.

(a) User Psychology: User psychology refers to all the attributes that are influenced by the user's mood or attitude (Ashbourn, 2004). Users may be wary of a new system – they do not trust it and are not aware of what happens

to their data in the background. A lack of trust in the system might deter the user from using the system correctly right from the enrolment stage. When it comes to mPayments, the user might be uncomfortable about storing his payment details on the mobile device, assuming that all the data will be lost and open to fraud in case the device is stolen. A nervous user might place his finger differently each time, resulting in false rejection. When using speaker verification, a nervous user could have a wavering voice or even a higher pitched voice and hence alter the speech print thereby resulting in a false rejection as well.

The best way to overcome these issues is to effectively communicate with the user (Ashbourn, 2004). Right from the enrolment stage, the user needs to be made aware of how the biometric mPayment application works, what data is being collected and why, what happens behind the scenes and how his data is secured – be it on the mobile device or in the central repository. Putting the user at ease from the beginning will help overcome the undesirable user perceptions. Existing applications can be used to demonstrate how fingerprint verification is used outside of the forensic sciences; examples like digiPROOF or even the unlocking of laptops could be used to inform the user of how the system is used otherwise. MPayment applications like Visa's payWave or MasterCard's PayPass could be used as well (both are described in Chapter 4).

(b) Individual Characteristics: Different individuals react differently to various biometric authentication techniques. As described in Section 5.1.1, Doddington's zoo classifies the user base into sheep, goats, lambs, wolves and chameleons. Ideally, we would want an entire user base of sheep – those who can easily adapt to the biometric authentication technique used; however, this is hardly the case. A person with small or extremely large fingertips may find it difficult to align his fingers on the fingerprint reader (Ashbourn, 2004). Other factors like age or even illness will also need to be considered: alternate arrangements will need to be made for people with disabilities. An alternate authentication mechanism will also be required in case the person has a wound on the finger.

Interestingly, speaker verification does not falter much with differing characteristics: (Ashbourn, 2004) says *"…subtle differences in the voice production mechanisms of males and females which, while perhaps typically producing a different waveform profile…do not seem to affect the operation of voice verification systems."*

(c) Usability: Usability refers to the ease of use with which the user can handle the application. This is again a factor that would apply to both the biometric side as well as the mPayment side of the application. The application should be user-friendly, intuitive and simple to use. As it competes with the simple handing over of a credit card or cash to make a payment, it should be as simple as possible. Keeping the biometric fingerprint reader on the mobile device minimizes the interaction of the user with external equipment to a minimum. The payment application should be a simple application that can be called up with the press of a button or that is automatically started up when it comes in proximity of the payment terminal at the POS (in the case of proximity payment). Also, the handling of the data should be easy too; the user should be able to add on new card details, top up payment credit or delete payment details easily from the mobile device. He should be able to view the list of recent transactions carried out. The fingerprint reader should be ergonomically placed – the user should not have to bend his fingers awkwardly to reach the reader; it should be robust enough for dirt and grime not to hinder a genuine verification. All these contribute to a pleasant payment experience for the user.

(d) Privacy: The issue of privacy is something that is of interest to all players in the value chain; not only do companies have to adhere to privacy rules, but they also have to ensure that the customer does not feel like his privacy is infringed upon.

Almost every industry offers some kind of a membership scheme where the user collects "points" of some kind; airlines, supermarket chains, car rentals, and on a smaller scale even cafés offer their customers loyalty cards with which they can collect points that can be redeemed for discounts, upgrades or

free goods[43]. While in its simplest form, these point collection schemes can be seen as mere CRM tools used to retain customers and ensure customer loyalty, it becomes a totally different picture when different stores partner or even offer a credit card in the context of the loyalty scheme[44]. That's when companies/ governments/organizations can potentially piece together (so-called profiling) the purchasing habits of a customer, indicating when he is where and doing what – a transparent customer. The level at which data is collected this day and age has made the user concerned about his privacy. As (Bohnet, 2009) states, users are not worried about the collection of the biometric data per se; the issue they have is more with what happens to the data afterwards and *its potential misuse*. The fear of becoming a transparent customer by linking all kinds of personal data to each other and profiling the customer is on the increase with advances in technology.

(Armington et al., 2002) classify privacy into **physical privacy** and **information privacy**. While information privacy refers to all the data that is being collected and stored, physical privacy refers to the customer having to use external biometric sensors, which he may be uncomfortable with because he considers it unhygienic or because of the criminal stigma attached to it. From a biometric mPayment context, privacy encompasses:

- Privacy of the biometric data
- Privacy of the payment data
- Privacy of personal data like name, address, bank account details
- Physical privacy in relation to the fingerprint readers

In a biometric mPayment application, the customer "gives out" both his biometric data as well as his payment data. Therefore, privacy would be a major concern from the user's point of view. Another aspect that influences consumer acceptance is Price of Convenience (PoC). PoC is a concept first introduced in 2002 (Ng-Kruelle et al., 2005). The idea behind PoC is that the customer pays a price – privacy – in return for a given service. Both the price "paid" and the convenience

[43] Examples: Airlines - Lufthansa Miles & More, Emirates Skywards; Supermarkets – Tesco Club Card (UK); Boots Card (Boots Pharmacy – UK); Starbucks Card (Starbucks Coffee)

[44] Payback Visa Card, Amazon MasterCard, Germanwings MasterCard

"received" are in a state of equilibrium. In a BiMoP application, for the convenience of using a secure mPayment application, the user agrees to giving price his personal as well as biometric data.

To put the customer at ease, it is important to inform him where his data is stored and what exactly happens to the stored data. The physical privacy issue can be minimized by using mobile devices with fingerprint readers on them.

5.3. Customer Acceptance – Issues in the area of Biometrics & mPayments

All of the above factors – technical, economic and human – affect the acceptance of the new application to varying degrees. While the technical factors may play a lesser role than the human factors, all of them are decisive in the overall acceptance of the payment application as they all contribute to the payment experience.

As mentioned earlier, customer acceptance – the willingness of the consumer to use the system – is crucial to the success of any new application. However technically brilliant a payment system may be, it will never be successful if there aren't sufficient users using it. Especially in the case of biometric mPayments, customer acceptance could possibly be difficult to achieve. Both technologies by themselves – mPayment and fingerprint verification –are mature, secure and established enough for reliable usage. However, both these technologies suffer from a lack of user acceptance. In the case of mPayments, this is primarily because the user does not feel the necessity for a new payment system and the perceived level of security. Unless the user sees some genuine advantage, he would not embrace a new payment system. On the biometric side, there is a criminal stigma attached to fingerprint verification.

Based on the idea that the customer acceptance is vital to the success of any new system, (Zmijewska et al., 2004) formulated a user-centric model which puts together the aspects that are pertinent to a user when it comes to mPayments. This

model was originally formulated for mPayments and is extended here to include the biometric aspect as well.

5.3.1. User-Centric Classifying Model

(Zmijewska et al., 2004) developed this model to understand the consumer's motivation and preference to use a new payment system. It is based on usability of the system which "*determines whether a consumer will start using an mPayment solution*" (Zmijewska et al., 2004).

The model uses a set of fourteen dimensions or categories. These dimensions are factors that are vital to the consumer's decision-making process about a new payment system. Analyzing the system based on these dimensions aid in understanding if a new payment system would potentially be accepted by the end-user.

Following are the fourteen dimensions as proposed by (Zmijewska et al., 2004).

1. **Change of phone requirement:** Consumers are generally wary of a payment system that required them to change their handset. If the benefits of the new handset outweigh the initial cost of changing handsets, they might consider it, but they commonly prefer not to change their mobile phone for the sake of being able to use a new payment system.

   To the disadvantage of mPayment systems using fingerprint verification, invariably all users would have to invest in new mobile handsets. Although there are mobile phones equipped with fingerprint sensors in the market at the moment, these are not widespread and not necessarily the first choice when a user selects a new handset.

2. **Registration requirement:** While some applications do not require an explicit registration/enrolment process, others do. According to (Zmijewska et al., 2004) users are more likely to use a payment system if that does not require enrolment and the disclosure of personal data.

Again, this dimension is not favourable to a BiMoP system. The enrolment process is vital for the accurate working of the verification process; moreover, collecting important data pertaining to the user is vital to ensure a secure system.

3. **Available phone operating company to which the user has to subscribe:** To reach a larger audience of customers, it is preferable that the payment solution is offered to customers of all MNOs rather than being MNO-specific. Seeing the payment system as a universal payment device increases customer acceptance than if it were something that were only available to a smaller group.

4. **Available applications:** In this context as given by (Zmijewska et al., 2004), an application refers to a utilization scenario where an mPayment system can be used. The more the number of utilization scenarios where the payment system can be used, the more likely it is to be accepted by the user. In other words, an ubiquitous BiMoP application would increase customer acceptance more than one that is specific to a certain utilization scenario.

   The BiMoP application as described in this thesis and illustrated in the business model in Chapter 6, proposes an ubiquitous payment system that can be used in almost all scenarios. While this is the proposed system, the actual implementation might take a few years. This is because not all POS terminals are equipped with NFC readers. Getting these readers to vending machines in all stores requires time and a certain amount of investment. It would be easiest to start with eCommerce and mCommerce scenarios along with popular brick and mortar chain stores and then slowly spread it out to other utilization scenarios.

5. **Communication of consumer's number to start transaction:** For an mPayment transaction, the customer invariably has to relay his mobile number to facilitate the transaction. This may be done actively by the consumer entering the number at the POS or may be automatically transferred by the

phone. To ensure an easy to use system, the consumer would prefer if this is done automatically.

In a BiMoP application, all the consumer would have to do is to authenticate himself using fingerprint verification and then let the data be transferred to the POS via NFC technology.

6. **Communication of transaction details to user:** For ease of use, the transaction details need to be relayed back to the mobile phone with minimal interaction from the user. The best option would probably be to save it in the mPayment application as in NGPay, India as described in Chapter 4.

7. **Acceptance of Transaction by Customer:** Customer Acceptance of a transaction refers to the customer authorizing the transaction. In most payments, the user authenticates himself and authorizes the transaction in the same action by entering his PIN. In a BiMoP application, the biometric merely replaces the PIN system and therefore would also be used to authorize the transaction.

   (Zmijewska et al., 2004) also stresses the importance of perceived security in the acceptance of a payment system. Although there are other factors that hinder the acceptance of a biometric-based system, the level of security would not be a problem.

8. **Confirmation to customer:** The user may place more trust in the system if he receives an instant confirmation that the payment has taken place. According to a study conducted by (Pousttchi, 2003), 89% of participants responded that this was important to them (Zmijewska et al., 2004).

   Most credit card transactions at store POS terminals provide this kind of instant confirmation. This should be possible in an mPayment system as well since the business model as proposed in this thesis would run on the existing payment infrastructure as used for card payments.

9. **Payment occurrence:** The payment occurrence refers to the way the transaction is settled between the customer and the payment provider. Existing methods are through the mobile phone bill, directly debiting the amount from the customer's bank account or deducting the amount from a prepaid value stored in the phone.

   In a BiMoP application the involved players need to decide how settlement takes place. If using an mPayment credit card transaction it might be best to leave settlement to the banks. In a multi-functional payment system that comprises an mWallet holding multiple cards as well as virtual cash, settlement might get more complicated; in such a case, the better option might be for the customer to settle all transactions via a single billing entity like the MNO.

10. **Brand visible to consumer:** Having a trusted brand offer the BiMoP application or just be associated with it could possible increase the customer's trust in the system and enhance the perceived level of security (Zmijewska et al., 2004).

11. **Value of payment:** Value of payment refers to the amount involved in the transaction – whether it is a micro-payment or a macro-payment. This also affects the customer acceptance of the payment application.

12. **Registration fee (yearly):** According to (Zmijewska et al., 2004), some payment systems charge a registration fee for the customers to start using the payment system.
    Apart from a registration fee, there is also the annual fee that some payment systems charge (credit cards for instance). While customers may not shy away from paying an annual fee as they do in the case of credit cards, this fee should be nominal.

13. **Transaction cost for consumer:** When using some mPayment systems the customer may have to incur certain additional costs involved with using the

application; for instance paying for an SMS message that communicates the payment detail from /to the phone.

The BiMoP application would use NFC technology to transfer data to the POS. Therefore, there are no data transfer costs that the user would have to incur.

14. **Time of transaction:** As explained under the technical factors in Section 5.2.1, the transaction time is very important to the customer. On an average, a credit card transaction takes less than 30 seconds (Zmijewska et al., 2004). The BiMoP payment system should be able to keep up within this time frame if not quicker. This would then provide the customer with a Value-Add to use the BiMoP system over credit cards.

The above fourteen dimensions represent the user-centric model used for classifying mPayments. These dimensions and their criteria can be applied to an mPayment application using fingerprint verification to assess the user's acceptance level of the new system. In Figure 14, the user-centric model has been applied for BiMoP applications; a colour coding scheme has been used to denote which dimension is in favour of BiMoP (indicated in green) and which are not (shown in red). It should be noted that this is only a model that assesses the likelihood of a new system being accepted by the user. It is not a guarantee.

The following table summarizes the fourteen dimensions and their criteria and also applies it to a BiMoP system using fingerprint verification. The fourteen dimensions have been applied to BiMoP application. A red/green colour coding has been used to indicate negative-positive influence of the dimension on the BiMoP application; for instance, since the user will have to upgrade to a mobile device with a fingerprint reader and potentially NFC technology, these have been labelled red, since the customer may not want to change to a new mobile device.

CATEGORY	CRITERIA	BiMoP
Change of phone requirement	None	
	Any WAP-enabled	
	New handset	
Registration requirement	None	
	Online	
	By Phone	
	In Person	
Available phone operating company to which the user has to subscribe	One	
	Several	
	All national Operators	
	Any	
Available applications	POS	
	Virtual POS	
	Mobile Merchant	
	Parking	
	Ticketing	
	Digital Content	
	Vending Machine	
	Utility bills	
	Pre-paid top-up	
	P2P	
Communication of consumer's number to start transaction	N/A - Initiated from the phone	
	Via Internet	
	Phone call	
	Scan device	
	Tell merchant	
Communication of transaction details to user	SMS	
	Voice call	
	Displayed on screen	
Acceptance of transaction by consumer	PIN	
	Session code	
	No special code required	
	Fingerprint	
Confirmation to customer	None	
	Paper receipt	
	SMS	
	Displayed on screen	
	Save to mWallet	
Payment occurence	From pre-paid account	
	From bank account	
	On phone bill	
	On credit card statement	
Brand visible to consumer	Mobile operator	
	Financial Institution	
	New brand	
Value of payment	Micropayments	
	Macropayments	
Registration Fee (yearly)	None	
	<= $15	
	> $15	
Transaction cost for consumer	None	
	Cost of phone call	
	SMS	
	Separate fee	
Time of transaction	< average cash transaction (10s)	
	< average credit transaction (30s)	
	30 sec - 1 min	
	over 1 minute	

Figure 14 – List of Dimensions from the User-centric Classifying Model

5.4. Carrying out Customer Enrolment – Appropriate Player

As can be seen from the examples in Chapter 4, there are a number of players involved in the business model of an mPayment application. There are the banks, the MNOs, merchants and the payment providers. While the payment provider can be an independent external party, it can also be a role that any of the other players can assume. While certain functions can easily be attached to certain players some cannot. The transmission of data for instance would be something that the MNO would take care of since that is his core competency. The bank would be best-suited to handle the financial aspects or a transaction as they have the necessary infrastructure. The question as to who could carry out the enrolment process is still an open one.

Looking back at the mPayment applications and the few biometric payment applications described in Chapter 4, a majority of the applications are offered by third party players and they are the ones that take care of the enrolment process. For pure mPayment applications, enrolment is simple usually taking place online with data being transferred to the mobile device. Between MNOs and banks, there are more banks – six of them – that carry out enrolment (be it online or within the bank) than the two MNOs. Although Pay by Touch closed operations, it remains a good example for this thesis as it combined mPayments and biometrics. Pay by Touch used an enrolment model where most of the details were captured through an application form online and the actual fingerprint template was captured at the POS terminal of the Pay by Touch merchant during the first purchase. This enrolment model carried out by Pay by Touch could be compared to the entry visa application process followed by embassies/consulates of the United States for instance where the applicant has to fill in an online application form that captures all relevant data like the name, address, passport details, employment details etc. After this is filled in, the applicant makes an appointment with the embassy for an interview and to capture the biometric template. This 2-stage enrolment process could potentially be a model that could be followed for biometric mPayment applications. However, rather than enrolling at a merchant terminal, it would be the banks/MNOs/payment provider that carries out the second stage of biometric data collection.

To a large extent, the player to carry out enrolment would depend on the business model, the kind of players involved and which player is the main provider of the mPayment application. Here we will only consider banks or MNOs as potential players to carry out enrolment.

5.4.1. MNOs

The Mobile Network Operator has an existing billing relationship with the customer and MNO personnel are more trained to handle mobile devices. Also, MNOs could easily enrol customers at the POS when selling them a new mobile device.

Where the actual authentication takes place could also play a role in deciding who takes on the enrolment process. If the actual authentication was to take place external to the mobile device, at the store POS terminal for instance, then it might be a better option for banks to take on the enrolment process. This is because there is an existing data transfer connection between the store and the bank and the fingerprint live template can be transferred along with the transaction details to the authorizing bank. However, in the model that this thesis proposes, authentication is carried out within the mobile device itself so as to minimize data transfer overhead and to protect the mWallet on the mobile device. In the long run, it is hoped that biometric mPayment becomes an ubiquitous form of payment than can be used anytime, anywhere. This means that the customer should be able to use it at a store POS, for online transactions, mobile transactions, at vending machines and even at ATMs. Providing authentication at the POS (or rather external to the mobile device) could mean that each of the different points of transaction – vending machine, store POS, computer, mobile phone – need to be equipped with a fingerprint reader. This would lead to tremendous costs and increases the risk of equipment being tampered with especially at vending machines.

A more simpler and “ubiquitous” method would be to secure the mWallet in the mobile phone with fingerprint authentication. This way most of the computation would take place within the phone. To pay, the customer would access his

mWallet and authenticate himself using his fingerprint. Then, the payment details would be transferred to the POS terminal using NFC technology as in the case of MasterCard PayPass. Such a system is less complicated to implement and more cost-effective as only the mobile device need be equipped with fingerprint readers. Also, it reduces the number of different readers the users would have to interact with, therefore reducing the FRR as the disparity in template samples from different readers is eliminated.

Even if a separate payment provider were to offer the mPayment facility, it would still be most feasible for the MNO to carry out enrolment: this would mean that the payment provider does not have to invest in new infrastructure required to carry out enrolment. MNOs usually have multiple stores in each city through which they market and sell phones and contracts. The MNO could use these premises to carry out enrolment. The personnel working for these MNO stores usually have in-depth knowledge about mobile devices and the security these devices provide. Therefore, minimal additional training would be required of them. Both bank and external payment provider employees would have to undergo specialized training to understand how the technology behind mobile phones works. Another reason, albeit a small one, is the fact that MNO stores are open for longer hours during the week than banks are; this lets users walk into their MNO store after working hours.

Another reason that speaks for MNOs to carry out enrolment is that they can directly market the BiMoP application to customers who purchase a new mobile device. If the customer decides to use the BiMoP application, he can directly enrol when buying the new mobile device. In its simplest form, this would be ideal for customers who would be using the mWallet just for storing cash. The cash credit to be stored on the phone can be uploaded into the device immediately with the customer paying the MNO. The storage of credit and debit cards gets a bit more complicated. This would require a few more questions to be answered:

- If the customer does not possess a credit card, does the MNO direct him to apply with his bank and request him to return with the credit card details or

can the MNO accept the credit card application on behalf of banks and pass them on for processing?

- Would the customer be able to use credit cards of all issuing banks in conjunction with mPayment? This would require a vertical alliance between all issuing banks and a horizontal alliance between the MNOs and banks.

- Would the MNO be authorized to convert the customer's payment cards to "mobile" cards? Would the customer by himself be authorized to enter his card details into the mWallet and start using them without informing the issuing bank?

5.4.2. BANKS

Banks enjoy a higher level of customer trust and seem to be in a good position to carry out enrolment since they already capture important customer data as well as perform a credit check on the customer. Banks have years of experience in payments and already offer various forms of payments like credit cards, debit cards, cheques, bank transfers and so on. They also have an existing relationship with merchants and the necessary infrastructure for payment transmissions.

Probably, the one advantage that speaks most for banks to carry out enrolment is the level of customer trust they enjoy. In the study conducted by (Wiedemann et al., 2008), 52.9% of the survey participants answered that they would prefer banks to be the provider of an mPayment application. 74% of the respondents said that they would use an mPayment application if it were offered by their own bank, while 58.5% of the respondents said they would use an mPayment application if it were provided by a renowned bank. However, (Wiedemann et al., 2008) continue to state that *"It can be deduced that, to a great extent, the preference for banks is based on purely subjective considerations of the user …(…)… and not necessarily on an objectively-based feeling of trust*[45]*."*

[45] Translation is author's own. Original text:
"Daraus kann abgeleitet werden, dass die Präferenz für Banken zu großen Teilen auf rein subjektiven Erwägungen der Nutzer, das heißt auf einem diffusen und nicht notwendigerweise objektiv begründeten Vertrauensgefühl, beruht." (Wiedemann et al., 2008, p. 100)

A table comparing the advantages of either the bank or MNO carrying out enrolment is shown in Figure 15.

Banks	MNOs
High level of Customer Trust	Existing billing relationship with customer
Already capture detailed customer data and perform credit checks on customers	Personnel trained to handle mobile devices
Payment is core competency	Easy in-store enrolment
Existing merchant partnerships	Better face-to-face relationship with customers

Figure 15 – Comparison of bank and MNO advantages (to provide enrolment)

A disadvantage that banks have is that their personnel are not trained to handle mobile devices, let alone enrol a biometric template using a mobile device. Although most banks have at least one branch in the cities where they operate, the target group of biometric mPayments is not necessarily a set of customers who visit their bank's branch to carry out their banking activities. Most of them use online or mobile banking for bank transfers and to view account status, have direct debits set up for bill payments and withdraw cash at ATMs. For any changes to their account, there is also the option of phone-banking. A visit to the branch is hardly ever necessary with these channels available. Given these, it may not be in the customer's or the bank's interest to carry out enrolment at a bank branch. Users are more likely to drop in at their MNO store for various reasons: to upgrade to a new mobile device with a new contract, to purchase additional equipment for their mobile devices or maybe in case of repairs to their mobile devices. The disadvantages of having either party carry out the enrolment process are given in Figure 16.

Banks	MNOs
Personnel will need training to handle mobile devices	Lesser customer trust when compared to banks
Step away from the otherwise automated banking model	
Opening hours are shorter when compared to MNO stores	

Figure 16 – Comparison of bank and MNO disadvantages (to provide enrolment)

As can be seen from the above two tables, both banks and MNOs have good reasons to be the player carrying out enrolment. The customer trust that banks enjoy should not be overlooked, however in terms of convenience, it might just be the MNO stores that are tailored for carrying out the biometric part of the enrolment process. Banks already store/own the payment data of customers; hence it would make sense to have banks own all the data rather than have it scattered between banks and MNOs. This would also put the customer at ease with regards to data privacy/security issues.

As mentioned earlier, a two-stage enrolment process as used by Pay By Touch is probably the ideal method to ensure a successful enrolment process where the customer is inconvenienced to a minimum. In the first step, the user would enrol online with his bank providing the required details like name, address, mobile number, name of MNO, as well as identification details. If the user is already enrolled for online banking, most details could be taken over. Once all details have been gathered, the user could then visit his MNO store; the staff at the MNO should be able to pull up the online application form with limited access – just enough to be able to verify name, address and verification credentials. The user would then get his biometric template enrolled and stored on his mobile device and the staff could confirm identity and ensure the user knows how to operate the biometric mPayment application. The data gathered during the second stage would be transmitted to the bank that carried out the first stage of enrolment.

6. Prospective Business Model for a BiMoP Application

The points discussed in this thesis can be tied together and depicted in a business model. A business model is essentially a framework that presents the significant aspects of a business idea. According to (Osterwalder et al., 2001), a business model, specifically one that is used in an eBusiness scenario, can be defined as "the architecture of a firm and its network or partners for creating, marketing and delivering value and relationship capital to one or several segments of customers in order to generate profitable and sustainable revenue streams."

From the above definition, the core aspects of a business model are:

(a) The actual service that produces value proposition from the customer perspective
(b) Organization of the player network
(c) Cost and revenue management
(d) Relationship capital.

The actual service that provides value proposition to the customer and the organization of the player network were discussed in Chapter 2. The intended service is a convenient and secure payment application using mobile devices; the organization of the player network is presented as a part of Pousstchi's MPRM model. How cost and revenue are managed within this network will not be delved into as it does not fall within the scope of this thesis.

Relationship capital is essentially the information resources and investments that serve the purpose of establishing good customer relationship. The concept of combining biometrics and customer relationship management (CRM) has been discussed by (Bohnet, 2009). Bohnet has defined CRM as: "…a long-term process that uses technology to support the goals of delivering customer satisfaction to produce long-term customer loyalty, and using smart investments to affect customer motivation and ultimately behaviour: if the customer won't use a new technology, it is a bad investment."

This definition sums up the key criteria for the success of a new technological innovation: for a new technology to be successful, the customer has to be willing to use it. In her book, Bohnet discusses how biometrics can be used to improve CRM for both the customer and the company[46]; in this context, biometrics is used as a tool to improve the relationship between the customer and the company. In BiMoP, biometric authentication is part of the product offered to the customer. A combination of these two ideas – using biometrics in the CRM process as well as for payments – would be taking a further step in the direction of an ubiquitous "instrument" that the customer can use to identify and verify himself.

Key to the success of BiMoP applications are customer acceptance and a working cooperative model between the different players; the cooperation between players is also necessary from the viewpoint of enrolment: using a two-stage enrolment process would require horizontal and vertical alliances between banks and MNOs.

For any business model, it is important to keep in mind the mission, structure, process and revenues associated with the business idea (Bouwman, Faber, Haaker et al., 2008). For the purpose of this thesis, we will follow the framework laid out by (Bouwman, Faber, Haaker et al., 2008) in the form of the STOF Model. The STOF model is then applied to formulate a business model for a biometric mPayment application.

6.1. The STOF Model [47]

The STOF model was designed to provide a theoretical framework for business models that caters specifically to mobile services. It looks at a prospective business idea from a service perspective; the driving force behind the model is the service/value that the new service provides to the customer.

STOF stands for **S**ervice, **T**echnology, **O**rganization and **F**inance. These four areas constitute the model and are known as domains. These domains are dependent on each other and each domain has a set of design variables that define

[46] Bohnet also discusses CRM from a government's perspective, but this does not relate to this thesis.

[47] Unless otherwise mentioned, STOF domains and design variables referenced from (Bouwman, Faber, Haaker et al., 2008) and the critical design issues from (Bouwman, Faber, Fielt et al., 2008)

the domain. Based on these variables are the critical design issues (CDI); the CDIs were derived from the analysis of case studies of existing mobile services. From the mPayment scenario, the cases that were analysed were Moxmo, Mobile2Pay and Mobipay (Bouwman, Faber, Fielt et al., 2008, p. 73). Finally, the STOF model has two critical success factors (CSF): customer value and network value. These measure the success of certain CDIs; as the application is still in its design phase, the CSFs will not be discussed further. To summarize, each domain in the STOF model is made up of:

- Design Variables
- CDIs
- Critical Success Factors

Essentially the STOF model consolidates and organizes all important features required to technically implement and market an mPayment application into the market into specific domains. The model – shown in Figure 17 – is described below and a business model for a BiMoP application is defined. It is assumed that the customer possesses a mobile phone equipped with a fingerprint reader.

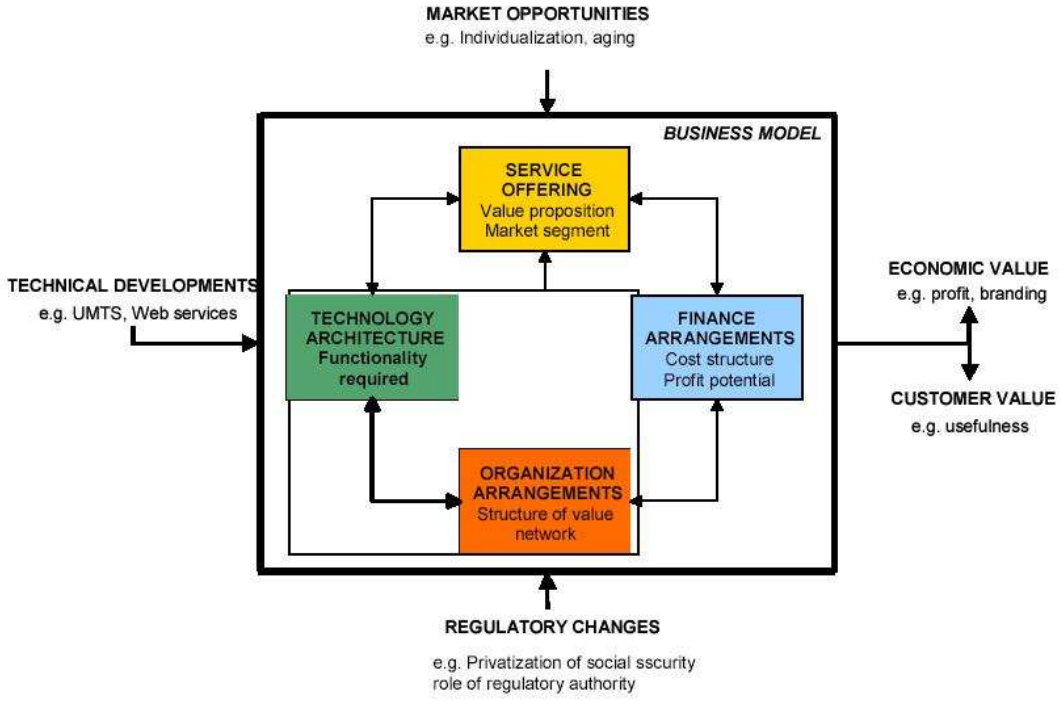


Figure 17 – STOF Business Model Framework (Bouwman et al., 2005)

6.1.1. Service Domain

As mentioned before, the STOF model takes a service-centric or value-centric approach in defining the business model. The focal point of the model is the value proposition that the offered goods/services hold (Bouwman, Faber, Haaker et al., 2008). Therefore, to define the service domain, four design variables that relate to value proposition are used. These are:

(a) Intended Value
(b) Delivered Value
(c) Expected Value
(d) Perceived Value

(a) Intended Value: Intended value is the value that the provider plans to offer to the end-user through the service/product. It is based on this value that the functional and technical specifications for the product are laid down. Consequently, the intended value affects the Technology Domain as well as the Organization Design.

The intended value behind a BiMoP application is to offer an mPayment application, which is more convenient to use than other available payment options, and to secure this using fingerprint verification.

(b) Delivered Value: The delivered value is the actual value that the end-user experiences. This could differ from the intended value. Although the provider may plan on offering a certain value/service to the end-user, the actual product itself may lose some of the specifications during the implementation process. As a result, the intended value and the actual delivered value may differ.

As the BiMoP application is still in the design phase, there is no delivered value to be described. The aim would be to be as close to the intended value as possible without compromising on factors like security and convenience. As the STOF model is dynamic in nature, the delivered value would flow into the business model when the application is launched.

(c) Expected Value: Expected value is what the end-user expects of the product. This expectation is usually based on factors like the offering company's reputation, trust in the company, financial aspects like cost of service or cost of the mobile device and the customer's previous experience with similar products/services.

To a certain extent, the value expected from a new payment application/option depends on the main player who is providing the payment option. The more the end-user trusts the player, the more "reliable" the end-user would expect the new payment option to be. In the business model as described here, banks would be offering the BiMoP application and hence the expected value could potentially be high.

(d) Perceived Value: Perceived value is what the customer eventually experiences; it is what value the user actually sees in the service/product. The perceived value depends on what the customer expects and the delivered value. The higher the delivered value or the lower the expected value, the higher the perceived value will be. Perceived value is what decides how successful a product will be; the better the perceived value, the more satisfied the customer will be and the better the penetration rate will be.

However sophisticated a product might be, if the user does not perceive it to be valuable, he is not going to use it. As mentioned in Chapter 1, the perceived security of mPayments is quite low. This in turn affects the value the end-user associates with the mPayment application. As the mPayment application will be using biometric authentication for security, the security apprehension could perhaps be reduced or even removed.

CDIs

Four CDIs were identified for the service domain; these are target group, value elements, branding and customer retention.

Target Group: It is important to identify the target group early on since the target group would hold a bearing in deciding the user requirements as well as marketing strategies.

While it is more and more younger people/adolescents who are tech-savvy and use the latest applications in the market, they may not necessarily be the appropriate target group for a BiMoP application. Their payment patterns usually lie in the micro-payment area; providing biometric security for a micro-payment may not be feasible from the perspective of the provider. Given this, the best target group to market a BiMoP application to would be the working population and even students with a steady income. Essentially, it would represent the same target group that is covered by credit card companies.

Value Elements: Depending on the target group, the value elements are defined. The value elements are essentially the characteristics of the service that are important to the end-user. This could be latest technology, speed, ease of use, fancy GUIs, trust, customer support and so on.
The value elements that a BiMoP application should provide are mainly convenience and security. The idea behind mPayment is to let the user make payments without using cash or plastic, thereby eliminating the necessity to carry around either of them; this makes mPayments more convenient than other payment options. Easy retrieval of data in case of loss or damage of the mobile device could be another potential value element

Branding: The issue of **branding** was found to influence the perceived value of the end-user (Bouwman, Faber, Fielt et al., 2008). As mentioned earlier in the thesis, trust plays an important role in customer acceptance of a new application. Therefore, offering a service under a brand name that the target group identify with or are familiar with could enhance chances of the success of the service.
The BiMoP application should be marketed by a player that the user trusts and is able to identify himself with. As banks enjoy a higher level of customer trust, they would be in the best position to market the BiMoP application under their brand, with MNOs as partners.

Customer Retention: Customer retention can be achieved using marketing strategies that keep the end-user satisfied. Retaining existing customers is usually much more cost-effective than attracting new ones; therefore, it is vital to ensure

that the customer is happy with the service provided. One way of achieving this is by providing adequate support to the end-user.

As it is a new application, the user may need assistance in the first few months of using the application. Also, there should be minimal technical difficulties and the number of false rejects and false accepts should be minimal, too. As an incentive, a loyalty scheme could be used that offers the customer certain benefits after a certain period of time of after he has made a certain number of payments with the BiMoP application.

6.1.2. Technology Domain

The specifications in the service domain are translated into technical structures; this is done in the technology domain. The required hardware, software and architecture is described in this domain. The following are the design variables of the technology design:

(a) Technical Architecture
(b) Backbone Infrastructure
(c) Access Networks
(d) Service Platforms
(e) Devices
(f) Applications
(g) Data
(h) Technical Functionality

(a) Technical Architecture: The technical architecture provides an overview of the technical design and ties together all the design variables in the technology domain. It also specifies whether the architecture will utilize:

- Centralized Vs. Distributed Architecture
- Open Vs. Closed
- Interoperable Vs. Non-interoperable

For a BiMoP application, the main question would be whether the application will follow a centralized or distributed architecture from the perspective of where the

biometric reference template is stored, where the payment details are stored and where the actual verification process is performed. **Storing the biometric data on the mobile device** eliminates the requirement of data transfer and would speed up the payment process. However, maintaining a central copy of the data would be helpful in the case of theft or if the user loses his mobile device. An idea might be for all the data to be stored on the mobile device while maintaining a central copy which is updated on a daily basis and which the user can manage, similar to online banking or the RBC Mobex web portal explained in Chapter 4. The next question that needs to be answered within the technical architecture framework is whether the system will be an open model or a closed model. To ensure that the BiMoP application is available to all users, an open system would be the most appropriate model, so that customers of all networks/banks/phone models can use the application.

(b) Backbone Infrastructure: This refers to the network infrastructure to be used. It encompasses network specifications, the kind of bandwidth used and similar characteristics.
The BiMoP application would be based on the existing card payment infrastructure for payment authorization.

(c) Access Networks: Access networks describe how the end-user would have access to the network – it decides whether the offered services will run on a fixed or wireless network, whether it will be accessible through hotspots and similar issues.
Being a payment system, the application should be available everywhere. Most of the payment data will be transferred over the payment infrastructure at the merchant's site. However, there needs to be a back-up plan in case either of these networks should fail.

(d) Service Platforms: This includes aspects like the technology used for billing, for CRM, authentication and all other middleware services. In the context of this thesis, the service platform variable is very significant as it is concerned with authentication.

All of these are vital aspects of a BiMoP application as they differentiate it from other payment options and give it a value-add. **Billing should be carried out by the provider of the payment application, which in this case is the bank**. Authentication is obviously done through fingerprint verification. The scope of CRM in such an application involving a variety of players is quite large and complex. While the primary responsibility might lie with the billing party as he is the one who has the relationship with the customer, all players need to be involved in CRM in some form or the other so as to maximize the benefits for the customer as well as the player.

(e) Devices: This refers to the devices required to use the product/service.
Being an mPayment application, the main device that will be used is the mobile phone itself. Other secondary devices that may be used are the POS terminals at the vendor site.

(f) Applications: This refers to the software required to run the product/service.
To provide a BiMoP application, an mWallet that handles the payment part as well as the biometric authentication software is required. Essentially the mWallet should be capable of storing payment data and comparing the biometric template to the reference template. It would be more cost-effective to outsource the software and then train in-staff members on how to use and support the system.

(g) Data: This variable describes how the data flow will be. It defines whether there is a data transfer requirement, if it needs to be real-time and the volume involved.
Most payment data transfer will take place at the merchant's POS terminal. Other data – like for instance update to personal data, addition of credit card details or addition of funds – can be added on the mobile device itself or online and synchronized with the central back-up copy.

(h) Technical Functionality: This describes the functionality offered by the technological system as a whole.

CDIs

There are five CDIs in the technology domain. These are security, Quality of Service, System Integration, Accessibility for Customers and management of user profiles.

Security: From the point of view of this thesis, security is the most important part. The issue and significance of security has already been discussed in Chapter 2; the perceived security of mPayments in very low. The use of fingerprint verification is meant to remediate this situation.

Quality of Service (QoS): QoS covers the delivery of the technical functionality as well as the support provided. It is distinguished by the support offered and the overall experience felt by the customer. Especially in a biometric application, the QoS offered is very important since the user is new to the technology and may need more assistance specifically during enrolment and in the initial phase of using the BiMoP application.

System Integration: System integration refers to the easy assimilation of the application into the existing facilities without the user having to change or add on new technology.

The BiMoP application should be easily integrated into the existing mobile device; the required software should either be already on the mobile device or it should be easily downloaded to the device at any later time. The hardware required for biometric authentication may be a problem; most mobile handsets available today are not equipped with a fingerprint reader. This would mean that users would have to invest in a new mobile handset, which they may not be willing to do. However, if speaker recognition is used instead, then there is less of a problem since all phones have the required microphones.

Customer Accessibility: The end-user should not have to have difficulty in gaining access to the new service: this defines customer accessibility.

The user should have easy access to the BiMoP application and the installation should also not be a problem. The easiest way to do this would be to have an application that can be easily downloaded onto the user's phone.

Management of User Profiles: The management of user profiles completes the list of CDIs in this domain. Creating a user profile should be easy from the user's perspective; privacy and data protection come into play here and a balance between access to the user's data and his privacy needs to be maintained.

Users should be able to manage their accounts as easily as they would in an online banking session. The user ID should be created during enrolment; the user should be able to easily add on new payment details either through an online portal, the mobile device itself. He should be able to set up one payment option from the mWallet – either one specific card or using prepaid cash value – as the standard payment option. In the study conducted by (Wiedemann et al., 2008), the respondents indicated that they would prefer to set up one payment option as the standard and change it in between if need be. Privacy was discussed in Chapter 5. Essentially, the customer needs to be ensured that his data – both payment and biometric – are secure and will not be misused. Similarly, personal privacy is ensured by keeping the fingerprint reader on the mobile device rather than a public one.

6.1.3. Organization Domain

The organization domain defines the network of players and their roles. A large part of the design variables in this domain have been described in Chapter 2, however not explicitly as design variables. The design variables are:

(a) Actors
(b) Value Network
(c) Interactions & Relations
(d) Strategies & Goals
(e) Organizational Arrangements
(f) Value Activities
(g) Resources & Capabilities

(a) Actors: As already discussed in Chapter 2, the actors are the various players involved in offering the service.

From a BiMoP perspective, the main players involved are the MNO and the bank. The bank will be the main payment provider who carries out enrolment and has the billing relationship with the customer; the MNO is in charge of the technical support for the mWallet including the collection of the biometric template. Other players like the mobile device manufacturer, who has to fit the mobile phone with the fingerprint reader, are more passively involved.

(b) Value Network: The value network defines the value chain between the various players and how they interact with each other.

The simple mPayment value chain network between the various players was discussed in Chapter 2. Implementing fingerprint verification in mPayments changes this value chain. This change starts right at the beginning with the registration/enrolment phase, which is carried out in two stages. The mPayment value chain as depicted by (Contius et al., 2003) is revisited here and the biometric factor will be applied to it. A major difference to the value chain is the order in which the different phases take place; in a biometric mPayment value chain, the authentication phase now comes before the initiation phase. Figure 18 depicts the new BiMoP value chain.

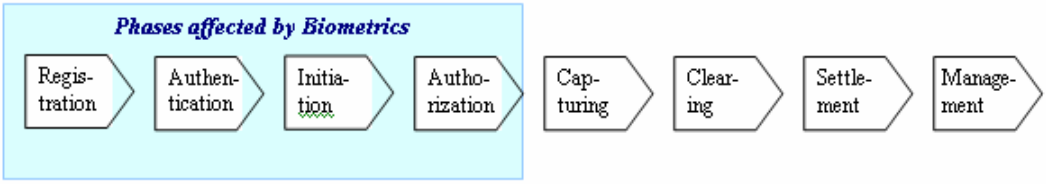


Figure 18 – The Biometric mPayment Value Chain (Own work based on (Contius et al., 2003))

Registration/Enrolment: While previously there wasn't the necessity for an explicit enrolment, it now is carried out in two stages – in the first stage the user's personal data is collected online and in the second stage the fingerprint template is collected. The user's identity needs to be verified and he needs to be trained to use the BiMoP application.

Authentication: Probably the biggest difference when compared to the mPayment value chain is the authentication phase. The actual replacement of contemporary authentication methods with fingerprint verification takes place in

this phase. Also, while in current mPayment applications, the authentication takes place after initiation, the authentication now is required to release the payment data to the merchant and is performed locally rather than on a central server. The authentication process becomes the first step in payment initiation.

Initiation: After authentication, the user now transfers the payment details to the merchant. This would equate to the initiation phase of the original value chain. In a BiMoP application as proposed in this thesis, this would incorporate transferring the data through NFC technology.

Authorization: The authorization process would function the same way as before. Should the customer be using a prepaid value stored in the mWallet, the authorization step would also be carried out in the mobile device and would only comprise of a check to see if the prepaid value can cover the transaction amount.

Capturing: The capturing phase remains unchanged too. There is the optional addition of transferring the transaction confirmation to the customer's mobile device. This would be done over the NFC interface.

Clearing: As clearing is entirely a back-end process, this phase remains unchanged.

Settlement: Settlement remains fairly unchanged too. In case of using prepaid cash value from the mWallet, there is no settlement; credit card transactions will be settled by the conventional credit card bill and debit card amounts will be deducted from the customer's bank account.

Management: The Management phase does not change either. It would still deal with all the post-settlement customer interaction. The player who is actually responsible for this phase would be the bank.

(c) Interactions & Relations: This variable defines the relationships between the various players. The interactions and relations that exist in a BiMoP application can be set at various levels; to simplify the interactions, it is best if the merchants work directly with their acquiring banks and the users directly with their MNOs/issuing banks.

(d) Strategies & Goals: In cases where there are multiple players involved in providing a new service, it is important to lay down contracts that specify the

legal obligations each party holds. This is because every player has a different core competency and therefore a different set of strategies and goals. To ensure that there is no opportunistic behaviour on the parts of the different players, there needs to be legally binding contracts and regulations laid down beforehand.
The strategies and goals of each player are not in the scope of this thesis and will therefore not be covered here.

(e) Organizational Arrangements: The more the number of players, the greater the interdependencies between them and the more complex the value chain gets. Due to this, the roles and responsibilities of each player needs to be clearly defined and an organizational arrangement needs to be mapped out.
The organizational arrangement lays out the roles and responsibilities of each player. These have already been laid out in Chapter 2.

(f) Value Activities: These are the activities that a player takes over in the value chain to deliver the required service.
The value activities have already been described under the value network; it specifies which player takes on which activity in the value chain.

(g) Resources & Capabilities: To build the value chain, the responsibilities, technical architecture, technical resources and capabilities are needed. These are defined in the resources and capabilities design variable.
The resources and capabilities of each player are not in the scope of this thesis and will therefore not be covered here.

CDIs

The CDIs in the organization domain are partner selection, network openness, network governance and network complexity with reference to the value network.

Partner Selection: Partner selection refers to the choice of other players in the network as well as whether different functionalities are outsourced or provided in-house.
As we are building on the existing credit card model, partner selection is simplified: the same set of partners are taken over from the credit card network,

with the addition of the MNOs, mobile device manufacturer and the software house providing the mWallet with fingerprint authentication.

Network Openness: Network openness refers to the ease with which a new player can join the existing value network.
For a BiMoP application, a walled garden model would be more appropriate. This ensures that the network of merchants and new banks or MNOs can join the network at a later stage making the application available to a wider range of customers as well as in a wider range of stores/services.

Network Governance: Which player takes on **network governance** is also an important question that needs to be answered. It was found that network governance was usually taken on by the player who developed the idea or who had direct access to the customer.
The best player to manage the network would be the bank since the bank is the player offering the BiMoP application.

Network Complexity: Network complexity refers to both the technical complexity as well as the complexity of the value network between players. All the players and their technical systems may need to be connected to each other and this could result in a very intricate network. As an example, in the case of credit cards, the merchants form part of the value network and add to its complexity. The credit cards firms reduce network complexity by designating the management of merchants to acquiring banks.
As mentioned earlier, the complexity of the network can be reduced by designated the management of merchants or acquiring banks for instance.

6.1.4. Financial Domain

As the name suggests the finance domain defines the financial structure required to offer the service/product. This consists of the associated costs, the investments expected by each player and the revenue sharing model. As the financial domain is not within the scope of this thesis, it will not be discussed in detail. The main points that would need to be decided before going ahead with a BiMoP project is to decide from where the capital for the investment is going to come from and

how much it will need to be. Also, the revenue sharing model will need to be decided upon. The most important design variable from this domain that we will discuss will be the pricing variable. The design variables are:

(a) Investment Sources
(b) Cost Sources
(c) Performance Indicators
(d) Revenue Sources
(e) Risk Sources
(f) Pricing
(g) Financial Arrangements

(a) Investment Sources: One of the most significant questions that need to be answered in the finance design is where the investment is coming from; the actual scale of the initial capital depends on the design choices made in the service and technology domain.

(b) Cost Sources: This refers to the costs involved in running the application; apart from the general fixed and variable costs generated in offering a product/service, there are also the costs involved in maintaining the value network.

(c) Performance Indicators: Performance indicators are required to make a judgement on how the product is doing in the market.. These kind of financial performance indicators include Return on Investment (ROI), market penetration rates, usage statistics etc.

(d) Revenue Sources: Revenue need not always come from the end-user; some services, especially those that are provided free of cost have other sources of revenue like for instance, advertising.

(e) Risk Sources: Sources of risk include the risk factors faced in offering the applications, including those that impact the other domains.

(f) Pricing: Whether and how the end-user is going to be charged for the services is laid down in pricing. As such, this is the only finance design variable that affects the end-user. Therefore, when deciding on pricing, factors like the target group and the existing payment models customers use have to be considered.
Pricing a BiMoP application is a difficult design variable to handle. Being a new payment application, the application needs to be priced low or even be offered free in order to appeal to customers. Especially so, since the user will have to invest in new handsets in the case of fingerprint verification. However, the entire value chain will also be investing in the new BiMoP application and hence would need to charge for the service in order to ensure a Return on Investment (ROI). The pricing could also follow the credit card model and charge the user an annual fee. In case of offering the payment free of charge, which would be ideal, the players may be able to receive revenue through other sources like advertising.

(g) Financial Arrangements: This is where the revenue sharing model, the cost sharing model and so on are described. From the point of view of the players, this might be the most significant finance design variable as it depicts how the profit and costs are shared between the various players.

The CDIs identified by (Bouwman, Faber, Fielt et al., 2008) affecting the finance domain are pricing, division of investments, division of costs and revenues and valuation of contributions and benefits. Pricing of the service should be such that the customer is willing to pay for the service while at the same time ensuring a profit for the value chain. As with any new service, there is a certain amount of risk and investment associated with the product. (Bouwman, Faber, Fielt et al., 2008) describe how companies have either outsourced the technical development of the product to reduce investment; another example the authors mention is the use of pilot projects that aid in gauging the interest and success rate of a new service/product to minimize risk. The valuation of contributions and benefits of each player is important in order to decide on a feasible revenue sharing model. The more the player contributes to the value chain, the more his share in the revenue model. The final CDI is the division of costs and revenues. While dividing the costs and revenues between the different players, each player's individual profitability as well as that of the network needs to be considered.

7. Summary & Conclusion

7.1. Summary

The concepts of mPayments, biometrics and how these can be combined to form a BiMoP application were discussed in this thesis. The factors that need to be considered – technical, economic as well as from the human perspective were illustrated and finally, a business model based on the STOF model was proposed, to tie it all together. The importance of player cooperation, customer acceptance and the perceived security were emphasized as aspects that could be decisive in the success of the BiMoP application.

To conclude, let us revisit and answer the research questions:

How is customer authentication done in contemporary mPayment applications?

Most mPayment applications in the market use PINs to authenticate the user. Geographic differences as well as the type of purchase made also influence the kind of authentication used.

- Most Indian mPayment applications seem to use a 6-digit PIN rather than conventional 4-digit PINs.
- Most mTicketing applications that are based on mPayment, like the RMV Hanau HandyTicket do not seem to have an explicit authentication process, probably because these are micro-payments with low risk.
- Only in very rare instances is biometrics used; Pay by Touch was an mPayment application that used fingerprint verification for authentication. While not an mPayment application, digiPROOF uses fingerprint verification to authenticate a user.

Is biometric authentication more suitable than contemporary authentication methods?

Present authentication processes work with no issues; however, the author suggests using biometric authentication for the following reasons:

- Contemporary authentication methods like PINs and passwords can be cracked and object-based authentication methods like tokens can be stolen. *A biometric cannot be cracked or stolen easily*. Hence, it is more secure.
- Convenience is another advantage that biometrics offer. PINs and passwords can be forgotten, just like tokens can be misplaced. *The user does not have to remember his biometric and cannot lose it* (unless through a physical accident).
- Biometric techniques enable better auditing of payment transactions. Biometrics cannot be transferred; this deters fraud and "buddy-punching".
- Being non-transferable makes biometric authentication powerful against repudiation. The user cannot deny having initiated the payment.

What factors should be considered during the biometric enrolment process?

Following factors need to considered for enrolment:

- An aspect that cannot be stressed enough is establishing the true identity of the person wanting to enrol. *"A user who enrols in a biometric system under a false identity will continue to have a false identity verified with every successful biometric match"* (Nanavati et al., 2002, p. 11).
- An alternate method of authentication is required in case the user is unable to use biometric authentication. People with injured fingers or disabilities should still be able to use mPayment; for such a situation, speaker verification could be used as an alternative.
- To ensure seamless enrolment, the customer needs to be well informed about the entire process: enrolment, the authentication, how mPayment works and what happens to his data behind the scenes.
- The threshold value needs to be variable depending on the customer. It will be based on the training samples acquired during enrolment.
- The personnel carrying out enrolment – the MNO store personnel in this case – need to be trained well to do this; they should be able to train the user how to place his finger on the reader; they should be able to differentiate the "sheep" from the "lambs" and consequently decide what threshold value to use.

- How the actual enrolment takes place needs to be decided. In this thesis, we recommend that it is performed in two stages: firstly, the online registration which captures all personal data like name, address, verification document numbers, mobile number, MNO and payment data; secondly, the enrolment of the biometric template which is done with the MNO. Even though the MNO performs the biometric enrolment, the bank would be the eventual owners of all data.

Which biometric is best-suited for use in mPayment? Why?

With ever decreasing mobile device size, the choice of the biometric suitable for mPayments is limited; fingerprint verification and speaker verification were found to be best for authentication in mPayments. The choice was made based on a set of technical, security and business factors as well as consumer acceptance, which are summarized into a criteria catalogue (see Chapter 3). These include:

- Device Size
- Size of Biometric Template
- Cost-effectiveness
- Response Time
- Enrolment
- Ergonomics
- User Perception

7.2. Conclusion & Future Outlook

Both mPayments and biometrics are not new technologies. mPayment applications have been surfacing for almost ten years; it was predicted that mPayments would become the standard form of payment within a few years. In 2010, mPayment as a payment option is pretty much still where it was ten years ago. There have been advancements in terms of technology with the introduction of NFC-based payment applications. However, other than for mTicketing, paying

using a mobile device is not as widespread as it was forecast to be. It is not the lack of technology that hindered the progress of mPayment, but more the:

- Lack of a standardized platform
- Lack of necessity for a new payment option
- Failure to be recognized as more a convenient mode of payment.
- Perceived level of security

In this thesis, mPayment meets biometrics in an effort to improve the overall security and the perceived security of an mPayment application. Biometric technology also comes with hindrances, one being the criminal stigma attached to it, especially fingerprint verification.

The BiMoP business model as described in Chapter 5 can only be successful if:

- Biometrics lose the criminal stigma attached to them. (Bohnet, 2009) gives two possibilities for biometrics to become a more mainstream authentication method: (a) With biometric authentication being enforced in immigration, border control and identification documents like passports and national IDs, the user may get accustomed to authenticating himself using biometric technology and (b) the user recognizes, by means of commercial applications like digiPROOF or even securing laptops, that biometrics improve their security and is more convenient to use. He starts to trust the system.

- The problem of having mobile devices equipped with fingerprint readers and NFC technology is resolved. Not all phones in the present market have these features. However, it is up to the MNOs to drive this; MNOs along with mobile device manufacturers can equip phones with these technologies. NFC technology could be used for various other forms of data transfer and fingerprint verification could replace the PIN used to unlock the phone as well as to secure other applications/data on the mobile device. With mobile devices becoming more than just phones and more like small forms of computers, users can secure confidential data, work-related material and possibly even IDs on their mobile device. It is up to the MNO to market these options as carriers of convenience making the mobile device the one-stop device that all

mobile device users carry on them anyway, and making it the only thing they need to carry around; eliminating wallets, cards and potentially even briefcases.

- MPayment is seen as a "**convenient necessity**". There is no doubt that mPayment is a convenient form of payment. The mWallet described in the business model eliminates the need for plastic, cash as well as loyalty cards. It eliminates the need for paper receipts as all transaction data can be stored in the wallet. The user will not need a wallet anymore. However, the customer needs to be convinced of all these; this will need to be done by the major credit card providers and driven through the issuing banks. If the big brands like Visa International, MasterCard and American Express market "plastic-less" credit cards and the mWallet under their brand logos and get a standard out that the issuing banks can follow, it would bring us one step closer to a successful BiMoP application.

There is a future for BiMoP. However, the future is not here yet.

Literature List

Armington, J., Purdy, H., & Koznek, P. (2002). *Biometric Authenticaiton in Infrastructure Security*. Paper presented at the Conference Name|. Retrieved Access Date|. from URL|.

Ashbourn, J. (2000). *Biometrics - Advanced Identity Verification: The Complete Guide* (2nd ed.). London: Springer Verlag.

Ashbourn, J. (2004). *Practical Biometrics - From Aspiration to Implementation*. London: Springer Verlag.

Bank of America. (2009). Photo Security. Retrieved 15th April, 2009, from http://www.bankofamerica.com/creditcards/index.cfm?template=cc_features_photo_security

Behrens, M., & Heumann, B. (2001). Fingerbilderkennung. In M. Behrens & R. Roth (Eds.), *Biometrische Identifikation - Grundlagen, Verfahren, Perspektiven* (1 ed.). Braunschweig/Wiesbaden: Vieweg Verlag.

Bimbot, F., Bonastre, J.-F., Fredouille, C., Gravier, G., Magrin-Chagnolleau, I., Meignier, S., Merlin, T., Ortega-Garcia, J., Petrovska-Delacrétaz, D., & Reynolds, D. A. (2004). A Tutorial on Text-Independent Speaker Verification. *EURASIP Journal on Applied Signal Processing, 4*, 430-451.

Bohnet, A. (2009). *Using Biometrics in Customer Relationship Management - Applications and Implications for Customers and Companies* (1 ed. Vol.). Saarbrücken: VDM Verlag Dr. Müller Aktiengesellschaft & Co. KG

Bolle, R., Connell, J. H., Pankanti, S., Ratha, N. K., & Senior, A. W. (2004). *Guide to Biometrics*. New York: Springer Verlag.

Bouwman, H., Faber, E., Fielt, E., Haaker, T., & De Reuver, M. (2008). STOF Model: Critical Design Issues and Critical Success Factors. In H. Bouwman, H. De Vos & T. Haaker (Eds.), *Mobile Service Innovation and Business Models* (pp. 71-88). Berlin Heidelberg: Springer Verlag.

Bouwman, H., Faber, E., Haaker, T., Kijl, B., & De Reuver, M. (2008). Conceptualizing the STOF Model. In H. Bouwman, H. De Vos & T. Haaker (Eds.), *Mobile Service Innovation and Business Models* (pp. 31-70). Berlin Heidelberg: Springer Verlag.

Bouwman, H., Faber, E., & Van der Spek, J. (2005). *Connecting Future Scenarios to Business Models of Insurance Intermediaries*. Paper presented at the Conference Name|. Retrieved Access Date|. from URL|.

Carpenter, H. (2008). Farewell, Pay by Touch, Farewell. Retrieved 5th Dec, 2008, 2008, from http://bhc3.wordpress.com/2008/03/19/farewell-pay-by-touch-farewell/

Chellam, R. (2005, 16.06.2005). Phishing scams seen surging this year. Retrieved 25.08.2005, 2005, from http://it.asia1.com.sg/newsdaily/news001_20050618.html

Chung, Y., Kim, K., Kim, M., Pan, S., & Park, N. (2005). *A Hardware Implementation for Fingerprint Retrieval.* Paper presented at the Knowledge-based Intelligent Information and Engineering Systems (KES 2005), Melbourne, Australia.

Contius, R., & Martignoni, R. (2003, 04.02.2003). *Mobile Payment im Spannungsfeld von Ungewissheit und Notwendigkeit.* Paper presented at the Mobile Commerce - Anwendungen & Perspektiven, Augsburg.

Creese, S., Goldsmith, M., Roscoe, B., & Zakiuddin, I. (2003, 12-14. March, 2004). *Authentication for Pervasive Computing.* Paper presented at the Security in Pervasive Computing, Boppard, Germany.

Currie, D. (2003). *Shedding some Light on Voice Authentication*: SANS Institute.

Dahlberg, T., & Mallat, N. (2002, June 6-8). *Mobile Payment Service Development - Managerial Implications of Consumer Value Perceptions.* Paper presented at the ECIS, Gdansk, Poland.

Dannenberg, M., & Ulrich, A. (2004). *E-Payment und E-Billing*: Gabler Verlag.

Daugman, J. (1999). Recognizing Persons by their Iris Patterns In A. K. Jain, R. Bolle & S. Pankanti (Eds.), *Biometrics - Personal Identification in Networked Society* (pp. 103-121). Boston: Kluwer Academic Publishers.

Ding, M., & Hampe, J. F. (2003, 2003). *Exploring Mobile Payments: The Rise and Fall of Paybox.*

Doddington, G. R., Liggett, W., Martin, A. F., Przybocki, M. A., & Reynolds, D. A. (1998). *Sheep, Goats, Lambs and Wolves*. Paper presented at the Conference Name|. Retrieved Access Date|. from URL|.

East Japan Railway Company. (2005). Mobile Suica. Retrieved 22nd Sept. 2008, 2008, from http://www.jreast.co.jp/e/press/20051101/

East Japan Railway Company. (2006). Four e-Payment Brands to Use Same Reader/Writer Retrieved 22nd Sept. 2008, 2008, from http://www.jreast.co.jp/e/press/20060902/index.html

ECBS. (2003). *Business and Functional Requirements for Mobile Payments*. Brussels: European Committee for Banking Standards.

ekey Biometric Systems. (2001). Ticketkauf mittels Handy und Fingerscan.

Eriksson, M. (2001). *Biometrics - Fingerprints based identity verification.* Unpublished Master Thesis, Umea University.

Finextra. (2005, 27.06.2005). European m-payments scheme SimPay collapses. *www.finextra.com*.

Fiutak, M. (2004). Koreaner launchen Fingerprint-Handy. Retrieved 04.04.2009, 2009, from http://www.zdnet.de/news/wirtschaft_sicherheit_security_koreaner_launchen_fingerprint_handy_story-39001024-39126068-1.htm

Fried, S. D., (CISSP). (2007). Enhancing Security through Biometric Technology. In H. F. Tipton, (CISSP) & M. Krause, (CISSP) (Eds.), *Information Security Management Handbook* (6 ed., Vol. 2, pp. 869-885). Boca Raton, FL Auerbach Publications (Taylor & Francis Group).

Furui, S. (1996). An Overview of Speaker Recognition Technology In C.-H. Lee, F. K. Soong & K. K. Paliwal (Eds.), *Automatic Speech and Speaker Recognition - Advanced Topics* (pp. 31-56): Kluwer Academic Publishers.

Gartner Inc. (2008). Gartner Says Worldwide Mobile Payment Users to Total 33 Million in 2008 [Electronic Version]. *2008 Press Releases*. Retrieved 20.09.2008 from http://www.gartner.com/it/page.jsp?id=652308.

GSMA. (2008). Global Mobile Awards History. Retrieved 4th October 2008, 2008, from http://www.globalmobileawards.com/history/index.shtml

Hagiu, A. (2006). Multi-Sided Platforms: From Microfoundations to Design and Expansion Strategies. Harvard Business School: Social Science Research Network.

Hammer, C., & Wieder, G. (2003). *Internet-Geschäftsmodelle mit Rendite*. Bonn: Galileo Business.

Hampe, J. F. (2004). Lecture: Wirtschaftsinformatik der Dienstleistungsindustrie: Zugangssicherung [Lecture]. Universität Koblenz-Landau.

Hampe, J. F., & Ding, M. (2003a, June 9-11, 2003). *Reconsidering the Challenges of mPayments: A Roadmap to Plotting the Potential of the Future mCommerce Market.* Paper presented at the 16th Bled Electronic Commerce Conference, eTransformation, Bled, Slovenia.

Hampe, J. F., & Ding, M. S. (2003b). *Changing Technological and Business Landscapes for mPayment. Is Local Mobile Payment Emerging as the Winner?* Paper presented at the Conference Name|. Retrieved Access Date|. from URL|.

Hampe, J. F., Swatman, P. M. C., & Swatman, P. A. (2000, June 19-21, 2000). *Mobile Electronic Commerce: Reintermediation in the Payment System.* Paper presented at the 13th International Bled Electronic Commerce Conference, Bled, Slovenia.

Hassler, V. (2001). *Security Fundamentals for E-Commerce*. Norwood, MA: Artech House.

Hazen, T. J., Weinstein, E., Kabir, R., Park, A., & Heisele, B. (2003, December 11-12, 2003). *Multi-modal Face and Speaker Identification on a Handheld Device.* Paper presented at the Workshop on Multimodal User Authentication Santa Barbara, California.

Henkel, J. (2001a, 16.08.2001). Bezahlen per Handy - viele Anbieter, aber noch kein Standard. *Frankfurter Allgemeinen Zeitung*.

Henkel, J. (2001b). Mobile Payment. In G. Silberer (Ed.), *Mobile Commerce*. Wiesbaden: Gabler Verlag.

Henkel, J., & Zimmerman, F. (2002). The Political Dimension of Payment System Innovations: The Case of Mobile Payments. *IPTS Report 63, Special Issue: e-Payment Systems Challenges for Europe*.

http://rbcmobex.com. (2009, 20th September, 2009). RBC Mobex™ Mobile Payment Service. from http://rbcmobex.com/

ICICI Bank. (2008). Ticket Booking - Book your Rail and Air Tickets Online. Retrieved 5th October 2008, 2008, from http://www.icicibank.com/pfsuser/icicibank/online/ticket_booking/ticket_booking.htm

International Biometric Group. (2005). *Global Biometric Market and Industry Report*. London: BITE.

International Telecommunication Unit. (2008). ICT Statistics. from http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#

Jansen, W. A. (2003, May 2003). *Authenticating Users on Handheld Devices.* Paper presented at the Canadian Information Technology Security Symposium.

JCB International. (2004). JCB's QUICPay Contactless Payment System Goes Mobile in Trial Starting November. Retrieved 20th Sept. 2008, 2008, from http://www.jcbinternational.com/htm/about/releases/20040914.htm

JiGrahak Mobility Solutions. (2008). www.ngpay.com. Retrieved 4th October 2008, 2008, from http://www.ngpay.com/site/index.html

Karlsson, J., & Taga, K. (2006). M-Payment im internationalen Kontext. In T. Lammer (Ed.), *E-Money, E-Payment & M-Payment* (pp. 73-87). Heidelberg: Physica-Verlag.

Karnouskos, S. (2004). Mobile Payment:A Journey through existing Procedures and Standardization Initiatives. *IEEE Communication Surveys & Tutorials, 6*, 44-66.

Kholmatov, A., & Yanikoglu, B. (2005). Identity Authentication using Improved Online Signature Verification Method. *Elsevier Pattern Recognition Letters, Letter 26*, 2400-2408.

Korczak, D. (2005). *Pilotstudie zur Überschuldung junger Erwachsener*: GP Forschungsgruppe, Institut für Grundlagen- und Programmforschung.

Koreman, J., Morris, A. C., Wu, D., Jassim, S., Sellahewa, H., Ehlers, J., Chollet, G., Aversano, G., Bredin, H., Garcia-Salicetti, S., Allano, L., Ly Van, B., & Dorizzi, B. (2006). *Multi-modal biometric authentication on the SecurePhone PDA.* Paper presented at the 2nd Workshop on Multimodal User Authentication (MMUA) 2006, Toulouse.

Kreyer, N., Pousttchi, K., & Turowski, K. (2002). *Standardized Payment Procedures as Key Enabling Factor for Mobile Commerce.* Paper presented at the EC-Web 2002.

Krueger, M. (2001). The Future of M-payments - Business Options and Policy Issues. *Electronic Payment Systems Observatory (*).*

Krueger, M. (2004). *Internet Zahlungssysteme aus Sicht der Verbraucher: Ergebnisse der Online-Umfrage IZV7*. Karlsruhe: Universität Karlsruhe.

LUUP.com. (2009, 12th March 2009). Deutsche Bank partners with Luup International to shape the future of mobile payments from https://www.luup.com/corporate/pressroom-press-deutschebank.html

Mallat, N. (2006). *Exploring Consumer Adoption of Mobile Payments - A Qualitative Study*. Paper presented at the Conference Name|. Retrieved Access Date|. from URL|.

Mallat, N., Dahlberg, T., & Öörni, A. (2003). *Trust Enhanced Technology Acceptance Model - Consumer Acceptance of Mobile Payment Solutions*.

MasterCard International. (2007). The NYC Mobile Trial. Retrieved 20th April, 2009, from http://www.mastercard.com/us/paypass/mobile/about/

MasterCard International. (2008). MasterCard PayPass. Retrieved 20th April, 2009, from http://www.mastercard.com/us/personal/en/aboutourcards/paypass/

MasterCard International. (2009). Blaze Mobile and MasterCard Worldwide Offer Innovative Payment Sticker for Tap & Go Payments Using Mobile Devices. Retrieved 20th April, 2009, from http://www.mastercard.com/us/company/en/newsroom/pr_blaze_mobile_and_mc_worldwide_offer.html

McKinney, M. (2008). Pay by Touch's backers claim fingers burned. Retrieved 5th December, 2008, from http://www.startribune.com/business/18182694.html

MHITs. (2008a). How It Works. Retrieved 5th December, 2008, from http://www.mhits.com.au/how-it-works.html

mHITs. (2008b). SMS payment provider mHITs launches Point Of Sale terminal. Retrieved 5th December, 2008, 2008, from http://www.mhits.com.au/releases/MEDIA_RELEASE_-_SMS_payment_provider_mHITs_launches_Point_Of_Sale_terminal_2008.pdf

Nanavati, S., Thieme, M., & Nanavati, R. (2002). *Biometrics - Identity Verification in a Networked World*. New York: John Wiley & Sons, Inc.

Ng-Kruelle, G., Swatman, P. A., Hampe, J. F., & Rebne, D. S. (2005). Biometrics and e-Identity (e-Passport) in the European Union: End-user Perspectives on the Adoption of a Controversial Innovation *Journal of Theoretical and Applied Electronic Commerce Research, 1*(2), 12-35.

Nokia. (2008). UK consumers want NFC on their mobiles Retrieved 20th April, 2009, from http://www.nokia.com/A4136001?newsid=1248102

NTT DOCOMO. (2008). Osaifu-Keitai. from http://www.nttdocomo.com/services/osaifu/index.html

O'Gorman, L. (1999). Fingerprint Verification. In A. K. Jain, R. Bolle & S. Pankanti (Eds.), *Biometrics - Personal Identification in Networked Society* (pp. 43-64). Boston: Kluwer Academic Publishers.

OMC Card Inc. (2006). *Introduction of QUICPay and Visa Touch Services.* Tokyo.

Ondrus, J., Lyytinen, K., & Pigneur, Y. (2009, 5-8 Jan 2009). *Why Mobile Payments Fail? Towards a Dynamic and Multi-perspective Explanation.* Paper presented at the 42nd Annual Hawaii International Conference on System Sciences (HICSS '09), Hawaii, USA.

Ondrus, J., & Pigneur, Y. (2004). *Coupling Mobile Payments and CRM in the Retail Industry.* University of Lausanne, Lausanne, Switzerland.

Osterwalder, A., Pigneur, Y., & Dubosson-Torbay, M. (2001). eBusiness Model Design, Classification and Measurements. *Thunderbird International Business REiew, 44*(1), 5-23.

Payment News. (2008). Pay by Touch To Shut Down All Biometric Services Immediately [Electronic Version]. *Payment News*. Retrieved 5th Dec, 2008 from http://www.paymentsnews.com/2008/03/pay-by-touch-to.html.

PC Welt. (2006). PG6200: Diebstahlschutz von Pantech mit Scanner. Retrieved 5th April, 2009, from http://www.pcwelt.de/start/mobility_handy_pda/archiv/53106/pg6200_diebstahlschutz_von_pantech_mit_scanner/

Phillips, J. P., Martin, A. F., C.L., W., & Przybocki, M. A. (2000). An Introduction to Evaluating Biometric Systems. *IEEE*, 56-63.

Polemi, D. (1997). *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, including an appraisal of the areas where they are most applicable* Athens: Institute of Communication and Computer Systems, National Technical University of Athens

Pousttchi, K. (2003). *Conditions For Acceptance And Usage Of Mobile Payment Procedures.* Paper presented at the mBusiness 2003 - The Second International Conference on Mobile Business, Vienna.

Pousttchi, K. (2004). *An Analysis of the Mobile Payment Problem in Europe.* Paper presented at the Mobile Business Systems, Mobile and Collaborative Business, Techniques and Applications for Mobile Commerce (TAMoCO), Essen

Pousttchi, K. (2005). *Mobile Payment in Deutschland - Szenarienübergreifendes Referenzmodell für mobile Bezahlvorgänge* (1 ed.). Augsburg: Deutscher Universitäts-Verlag.

Rannenberg, K., Albers, A., Figge, S., Radmacher, M., & Rossnagel, H. (2005). *Mobile Commerce - Forschungsfragen am Scheideweg der Mobilfunkgenerationen.* Paper presented at the MCTA 2005.

RCMP. (2002). *Biometric Technologies: An Assessment of Practical Applications*: RCMP Technical Security Branch.

Rila, L. (2002, October). *Denial of Access in Biometric-Based Authentication Systems.* Paper presented at the Infrastructure Security: International Conference, InfraSec 2002, Bristol, UK.

RMV. (2008). Get>>In, das intelligent Hanau-Ticket.

Roche, J. (2002). *Mobile Trading Comes of Age*. Paper presented at the Conference Name|. Retrieved Access Date|. from URL|.

Royal Canadian Mounted Police. (2002). *Biometric Technologies: An Assessment of Practical Applications*: RCMP Technical Security Branch.

Scheuermann, D., Schwiderski-Grosche, S., & Struif, B. (2000). *Usability of Biometrics in Relation to Electronic Signatures* (No. 118): GMD - Forschungszentrum Informationstechnik GmbH.

Schmidt, C., & Lenz, J.-M. (2001). Unterschriftenerkennung. In M. Behrens & R. Roth (Eds.), *Biometrische Identifikation - Grundlagen, Verfahren, Perspektiven* (1 ed., pp. 179-193). Braunschweig/Wiesbaden: Vieweg Verlag.

Skinner, C. (2008, 18/01/2008). Why mobile banking doesn't work ... yet. Retrieved 4th April, 2009, from http://www.finextra.com/community/fullblog.aspx?id=869

Statistics Bureau Japan. (2007). *Statistical Handbook of Japan*.

Stroborn, K., Hinrichs, J.-W., & van Baal, S. (2004). *(Mobiles) Bezahlen aus der Sicht des Online-Händlers: Status Quo und Perspektiven.* Paper presented at the Mobile Economy - Transaktionen, Prozesse, Anwendungen und Dienste, Universität Augsburg.

Teletrust e.V. (2002). *Bewertungskriterien zur Vergleichbarkeit biometrischer Verfahren*

Telstra. (2009). Australia's first contactless mobile payment trial rings in success. Retrieved 5th April, 2009, from http://www.telstra.com.au/abouttelstra/media/announcements_article.cfm?ObjectID=44463

Thiel, C. (2002). Anforderungen an biometrische Systeme aus bankenfachlicher Sicht. In V. Nolde & L. Leger (Eds.), *Biometrische Verfahren* (pp. 313-321). Köln: Deutscher Wirtschaftsdienst GmbH & Co. KG.

Tilton, C. (2006). The Role of Biometrics in Enterprise Security: www.dell.com/powersolutions.

UK Biometrics Working Group. (2002). *Use of Biometrics for Identification and Authentication - Advice on Product Selection*: Biometrics Working Group.

US Bureau of Consular Affairs. (2009). Visa Waiver Program - FAQ [Electronic Version]. Retrieved 8th September, 2009 from http://travel.state.gov/visa/temp/without/without_1990.html.

Visa International. (2009). Visa Contactless – the 'wave and pay' alternative to cash for low value transactions. Retrieved 20th April, 2009, from http://www.visaeurope.com/pressandmedia/factsheets/visacontactless.jsp

Weng, J. J., & Swets, D. L. (1999). Face Recognition. In A. K. Jain, R. Bolle & S. Pankanti (Eds.), *Biometrics - Personal Identification in Networked Society* (pp. 65-87). Boston: Kluwer Academic Publishers.

Wiedemann, D., Goeke, L., & Pousttchi, K. (2008). *Ausgestaltung mobiler Bezahlverfahren - Ergebnisse der Studie MP3*.

Wikipedia. (2007). Osaifu-Keitai [Electronic Version]. *www.wikipedia.org*. Retrieved 03.02.2008.

Wolf, A., & Tacke, J. (2003). *Authentifizierung durch Sprache - Potenziale und Grenzen biometrischer Systeme*. Paper presented at the "Security, E-Learning, E-Services" 17. DFN - Arbeitstagung über Kommunikationsnetze, Düsseldorf.

Woodward, J., Orlans, N., & Higgins, P. T. (2003). *Biometrics - Identity Assurance in the Information Age*. Berkeley California: McGraw-Hill.

Wray, R. (2006). UK: Scramble Starts for Pay-by-Mobile Business [Electronic Version]. *www.paymentnews.com*. Retrieved 13 October, 2006 from http://www.paymentnews.com/2006/05/uk_scramble_sta.html.

www.bahn.de. (2008). Ein Fahrschein – viele Möglichkeiten: Die Fahrkarten-Buchung der Bahn.

www.chip.de. (2008). P960: Erstes Handy von Lenovo. Retrieved 04.04.09, 2009, from http://www.chip.de/news/P960-Erstes-Handy-von-Lenovo_32503440.html

www.coolstuffjapan.sblorgh.org. (2007, 05.09.2007). The Cool Stuff in Japan Guide. Retrieved 20.09.2008, 2008, from http://coolstuffjapan.sblorgh.org/mobile_phones/edy/

www.edy.jp. (2008). About BitWallet (Company Profile). Retrieved 20th Sept. 2008, 2008, from www.edy.jp

www.gsmdome.com. (2009). Fujitsu F-01A Is a Waterproof Phone, Packs a Fingerprint Scanner Retrieved 04.04.09, 2009, from http://www.gsmdome.com/ntt-docomo/fujitsu-f-01a-is-a-waterproof-phone-packs-a-fingerprint-scanner_3313

www.inside-handy.de. (2006). Pantech PG 6200: Handy scannt Fingerabdruck des Besitzers. Retrieved 4.04.09, 2009, from http://www.inside-handy.de/news/6564.html

www.mchek.com. (2008). mChek/Payment: Frequently Asked Questions. Retrieved 4th October, 2008, 2008, from http://www.mchek.com/popUp_faq.htm

www.nets.com.sg. (2008). NETS, SingTel and UOB Launches Near Field Communications (NFC) Public Trial.

www.ngpay.com. (2008). NgPay Partner FAQ IRCTC - Indian Railways Booking. Retrieved 5th October, 2008, 2008, from http://www.ngpay.com/site/faqs_irctc.html

www.paymate.co.in. (2008). PayMate. Retrieved 4th October 2008, 2008, from www.paymate.co.in

Zinke, J. (2001). Sprechererkennung. In M. Behrens & R. Roth (Eds.), *Biometrische Identifikation - Grundlagen, Verfahren, Perspektiven* (pp. 159-178). Braunschweig/Wiesbaden.

Zmijewska, A., & Lawrence, E. (2006, January 23-25, 2006). *Implementation Models in Mobile Payments.* Paper presented at the Advances in Computer Science and Technology (ACST 2006), Puerto Vallarta, Mexico.

Zmijewska, A., Lawrence, E., & Steele, R. (2004). *Classifying m-payments - A User-centric Model.* Paper presented at the 3rd International Conference on Mobile Business.

Declaration

I, Shiny Sreekumar, herewith declare that

“Biometric Authentication in Mobile Payments”

is my own original work and that all sources I have used or quoted have been indicated and acknowledged by means of complete references.

_____

Location, Date

_____

Signature