

1 INTRODUCTION

With the growing prevalence of the electronic commerce and the widespread use of mobile phones, a new type of channel is emerging, called mobile commerce, or m-commerce. The use of e-commerce has already digitalized the payment process, so physical contact between the buyer and seller is no longer necessary. The conversion from physical to virtual payments has brought enormous benefits to consumers and merchants alike [1]. Moreover, mobile commerce will likely require real-time cashless mobile payments for buying physical and digital goods anywhere at anytime. The immediate consequence is a race between payment service providers such as banks, card companies and mobile network operators to be the first to offer a new successful mode of virtual payments. However, some recent analysis shows that mobile payment has not proven to be a source of competitive advantage for neither financial institutions nor for mobile operators [2]. Hence, the current tendency for each actor is to try to pick the right business model to maximize their market share rather than trying to lead the market.

Mobile payments, defined as payments carried out wirelessly via a mobile device, are likely to become an important section of the retail payment sector [3]. Gartner Research predicted that the transaction value of mobile payments will expand to \$15 billion in Western Europe by year-end 2005 [4]. In an attempt to overbid this forecast, Forrester Research, predicted that mobile payments will amount to only 26 billion euro in 2005 – 87 euro per mobile phone user per year -- and just 0.5% of consumer spending, excluding housing and vehicle purchases [5]. However, mobile payment is confronted with technological and business issues that delay its development. The biggest challenge that mobile payment providers face at this time is convincing European consumers and merchants that they need new payment systems [6].

The current slow start of m-commerce can be attributed to the fact that it suffers from the same problems troubling e-commerce, plus a few of its own [7], such as device

and network limitations, maturity of payment solutions, and customers' lack of interest [8]. Nevertheless, according to Durlacher Research, the potential of m-commerce remains enormous, predicting that the market could be worth 26 billion euro in Europe by year 2005 [9]. This has prompted many mobile and financial industries to claim that it is time to promote mobile payments in order to accelerate the development, acceptance and use of the m-commerce.

Another way to explain the real enthusiasm around m-commerce would be the penetration of mobile phones estimated in Western Europe reached almost 70% by the end of 2003 [10]. Moreover, the arrival of the new 3G services that will be coming with UMTS addressed some disabling problems and deliver more possibilities for new mobile applications, which will need a good payment system. Consequently, we expect that more people might want to make payment transactions over their mobile handset. Some recent Gartner survey data indicates that approximately 46% of Western Europeans already use a mobile device for making some kind of mobile purchase [4] (e.g., news alerts, logo, ring tones). The types of mobile device that can be used for m-commerce range from the classic mobile phone, PDA and laptop, to more surprising devices such as refrigerators and cars. The growing need for ubiquity and mobility promises a bright future for m-commerce, which creates an environment where consumers and merchants are able to conduct business anywhere, anytime and any way they like. Herzberg insists that security and convenience are two essential properties that mobile devices should have [11].

The mobile telecommunication area is subject to an important debate which concerns the current and future successful technology in m-commerce. Mobile voice is quickly becoming a commodity and mobile operators are increasingly looking for ways to reduce the loss of subscribers to cheaper competitors and at the same time open up new revenue streams. Offering mobile electronic commerce services is a way of achieving both of these goals. The enabling technology is rapidly advancing and operators must act now to become central player in this lucrative market. It has been observed that mobile voice telephony (e.g., GSM, GPRS, UMTS, ...) and data communication (e.g., WLAN, Bluetooth, infrared, RFID, ...) are converging to offer the same type of services. Sooner or later, the telecommunication market will change

in the sense that one type of network will be able to handle voice conversations and data transfers with good quality of service. The objective is to respond to the desire of increased mobility, whether for carrying voice or data.

Some mobile network operators are preparing to compete on both markets. For example, Swisscom bought a UMTS license to offer 3G services, but they are also promoting WLAN hotspots. Today, these technologies are different enough to be complementary, especially concerning the speed of transmission and coverage. However, in the future, we cannot be assured that the distinction will be so evident.

In this paper, we give a general overview of the mobile telecommunication sector. In addition, we review different payment mechanisms to obtain a better understanding of the impact of mobile payments. Therefore, the current and emerging technologies behind m-commerce is investigated and the elements needed in an advanced m-commerce service platform are looked at. Also we propose to use some description, classification and decomposition tools for existing payment systems and technology. Furthermore, we identify the actors in the mobile payment arena and the various strategies and technologies that these actors can choose. As a result all this contribution gives an overview of the experiences gained and practically applied in a case study: “Mobile Banking Service Project”; which presents some results achieved so far.

2 MOBILE WORLD

2.1 Mobile Telecommunication

There are about four times as many mobile phone subscribers in Europe as there are Internet subscribers, and penetration rates are still climbing. In some business sectors, penetration is total. When SAS surveyed its executive club, it found that while about half of the members had a PC, every single one of them had a mobile phone. The mobile phone is undergoing a transition from a voice device to a general-purpose e-commerce device and the same time as the technology shifts from low-speed to high-speed data services. The combination should be irresistible to many service providers, and banks are no exception. Given this vision, we must be sure to found corporate strategies on the infrastructure that will be in place in the near future and no restrict thinking about e-commerce to models built around web pages and credit cards. For many organizations, in fact, the mobile phone and not the web should be the priority for building an effective customer relationship.

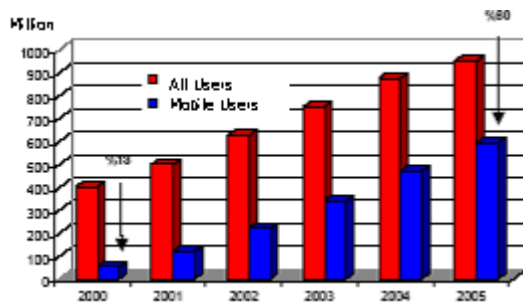


Figure 1: Mobile Users at Web

Source IDC Internet Commerce Market Model,V7.1

Forrester Research supposed at 2000 that usage of information technologies at Europe would be as shown as Table 1. The graphical appearance of these data is as given at Figure 1. At this point, Forrester Research has an idea that the electronic commerce market is to be approximately 4 trillion dollar, and also one of the three European has an access to the Internet. [12]

Table 1: Usage of Information Technologies at Europe Numbers as abbreviated for million and collected from the users from Sweden, Holland, Germany, England and French where are older than 16. Source: Forrester Research, 2000

	1999	2000	2001	2002	2003
Average Population	178,2	178,8	179,5	180,3	180,9
PC Users	64,2	69	73,4	78,5	83,7
Internet Users	33,9	40,3	46	50,8	58,7
Digital Tel. Users	49,8	62,7	76,1	87,9	98,7
TV Connections	8,2	11,2	13,7	17,3	21,3

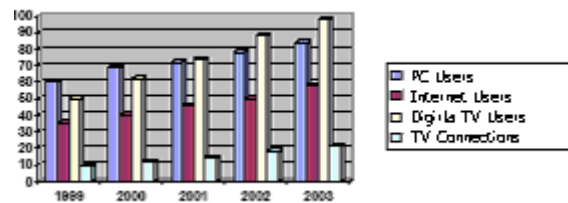


Figure 2: Usage of Information Technologies at Europe

Recently, there is no statistical information about the value for the e-commerce market in Turkey. However at 1999, 7 million dollar e-commerce share is supposed to increase to 840 million dollar at 2003, and 6 billion dollar at 2005. In our country, electronic banking and marketing is a tool for mostly online shopping, online ticket reservation, on-line sale for electronic equipment etc. This gives the clue that the electronic market has a real attempt in Turkey. Hewlett Packard projected that in 2003 Turkey made the 50 percent transactions between companies over the net.[13]

2.1.1 Mobile Telecommunication in the World

Mobile telecommunication market is the world's fastest growing market. As of today there are approximately 470 million mobile telecommunication subscribers and this number is estimated to reach 700 million by 2004 and 1.3 billion at the end of the following 5 years. According to another estimation there are already 700 million

mobile phone users[17]. In U.S. it is stated that mobile telecommunication population has gone beyond 35% and the number of radio communication subscribers is over 100 million. The companies in the market have nearly 150.000 employee and make their country earn a revenue over 44 billion US Dollars [18].

In a report prepared by UMTS Forum [19], it is stated that the Forum outsources Analysis and Intercai research firms to work on a conjecture over UMTS market and according to this conjecture, the telecommunication population will reach 50% in the following 10 years. In the same report, it is stated that West Europe mobile market will reach 130 million subscribers by the end of 2001 and this number will be 200 million by the end of 2005[20]. Again in the same report it is stated that, in Europe, mobile multi-media subscriber number will be 32 million by the end of 2005 which means a 34 billion ECU (including services, terminal devices) revenue per year [21].

According to the subject, to project a conjecture for the Europe's long run trend, UMTS Forum states that for 2015 the Europe mobile market will have 300 million subscribers and mobile market will be mature about 2017.

According to a recent report prepared by the EU [22], EU telecommunication services market has a value of 200 billion ECU as of today and has a progressive growth of 12.5% per year. It is stated that the mobile communication sector, which has a growth of 38% in 2000, has a share about 30% in the EU telecommunication services sector's total revenue.

In Europe, the mobile subscriber density is higher with respect to PC user density. Because of this, by the start of 3G services it is anticipated that mobile phone will be the one to chosen for Internet access and e-commerce among the other devices. Although in U.S. the PC user population and Internet usage ratio are high with respect to mobile phone usage, by the start of Internet access over mobile phones will increase the tendency of people to buy mobile phones. In other words by the 3G technology usage, mostly mobile phone using Europeans will use mobile phones to access Internet rather than PC's. Nevertheless, it is estimated that mostly PC user Americans will tend to buy more mobile phones for their Internet access. Briefly, both in US and Europe, if the attributes like; service price, quality, usability and

security don't progress in the unfavorable way it is stated that the mobile phone usage will easily increase.

In the table below, the number of mobile telecommunication subscribers all around the world regions is described with respect to reached/planned values (referenced by the end of the years mentioned in the rows).

Table 2 : The number of subscribers in Mobile Telecommunication Sector (based on region vs. year)[23]

Region/Year	1995	2000	2005	2010	2015
EU 15	22	113	200	260	300
South America	36	127	190	220	230
Asia Pasific	22	149	400	850	1400
Other	7	37	150	400	800
Summary	87	426	940	1730	2730

2.1.2 Mobile Telecommunication in Turkey

Turkey have met mobile telecommunication sector by the usage of “Nordic Mobile Telephone” (NMT) in 1986. As of today by NMT approximately 114000 subscribers are serviced. Also in 2G technology field, Turkey has 4 GSM service providers as Turkcell, Telsim, Istim and Turk Telekom. Turkcell and Telsim have been providing GSM900 services since 1994 by the revenue sharing contract made with the Turk Telekom. By the changes in the scope of current law about the firms of the subject to be given licence, in 27April 1998 a contract was signed between ministry of Communications, Turkcell and Telsim.

By April 2000, awarding of GSM1800 has been started and as the awarding has been eventuated in 30th September 2000 a contract between Istim and ministry of Communication has been signed. And by 21st March 2001 Istim started as a service provider.

Turk Telekom is the other GSM1800 service provider in Turkey and by the same contract about GSM1800 licence, a contract was also signed between ministry of Communication and Turk Telekom. But Turk Telekom has not started providing this service yet.

The two GSM service providers Turkcell and Telsim are in preparation for 3G technology that Turkcell has attended Ericsson and Telsim has attended Siemens/Motorola for the required technology infrastructure[24]. Telsim has signed a contract with Motorola in August, 2000 for the development of new 3G technologies and also signed a UMTS Platform construction project which has a potential cost of 2billion US Dollars[25].

According to the 8th five years progress report which includes the period 2001-2005 prepared by Government Planning Organization[24], by the presence of Turkcell and Telsim end of year 2000 subscriber number is 12million and subscriber density have reached 17%.

Again according to this plan, it is proposed that by the result of tendency towards mobile telecommunications services and the fast development in the market's lowering the cost, the fast development of the market will continue. In the following period, it is proposed that, most of all Internet access and e-commerce and the other many telecommunication services will use mobile networks.

DPT proposes that, also in this period 3G mobile systems will start functioning and the systems aforementioned will intensify mobile structured telecommunications. In the plan it is estimated that mobile phone subscriber number and its density will reach 30.5 million and 44% respectively.

2.2 Mobile Data

The data capabilities of the mobile platform are expanding. Data rates reach 144Kb/s with the introduction of the Universal Mobile Telephone Service and will then move on to 2Mbits/s by 2005. UMTS is the latest world-wide standard for mobile phones: NTT DoCoMo in Japan recently placed the first commercial order for UMTS equipment and launched their new (\$16 billion) network in 2001. While the higher speeds of UMTS were a year or two away, interim solutions found to push GSM data

rates up to 28.8Kb/s with High Speed Circuit Switched Data (HSCSD) and improve interactive capabilities with the transactional SMS service known as Unstructured Supplementary Service Data (USSD). Data rates then quickly moved on to a maximum of 115Kb/s with the "always on" General Packet Radio Service (GPRS). Most European operators had already deployed GPRS until the end of 2003. This was soon followed by the deployment of Enhanced Data for the GSM Environment (EDGE), providing services at up to 384Kb/s. This was the entry point for "3rd Generation" services and the first meeting of the Third Generation Partnership Project (3GPP) took place in October: Members include the four major industry bodies (GSM Association, Global Mobile Suppliers Association, the Universal Wireless Communications Consortium and the UMTS Forum) as well as the standards bodies for Europe (ETSI), China, Japan, Korea and the USA.

The first big step in Europe was GPRS. GPRS is an 'always on' connection to mobiles that is far faster and more reliable than existing circuit-based connections. In the UK, Cellnet introduced GPRS across its network in 1999 and is already talking to customers about the applications they might use GPRS for, and the type of terminals or handsets they need. GPRS can provide data speeds of up to 115 kilobits per second [20]. In Turkey, emerging mobile operators Turkcell, Telco, and Telsim introduced GPRS at the end of the 1999.

The trend here is clear: digital mobile isn't just about interpersonal voice communications. Since organizations are rolling out vertical applications built on mobile devices, ranging from RAC engineering reports to Community Health Trust patient records, the perception of the mobile handset is about to change. Instead of being seen as nothing more than a convenient means of making voice calls, the transaction will be seen as an indispensable integrated 'umbilical cord' for personal.

2.3 Mobile Technology

2.3.1 Technology Transitions

Electromagnetic waves were first discovered as a communications medium at the end of the 19th century. The first systems offering mobile telephone service (car phone) were introduced in the late 1940s in the United States and in the early 1950s in

Europe. Those early single cell systems were severely constrained by restricted mobility, low capacity, limited service, and poor speech quality. The equipment was heavy, bulky, expensive, and susceptible to interference. Because of those limitations, less than one million subscribers were registered worldwide by the early 1980s.

Inexpensive phones with built-in facilities and applications and lower per-call rates have made mobile services an essential part of life for many users. Business and commerce rely heavily upon mobile services, and many job entrants, students, and young people use cellular phones as their primary telephone.[21]

2.3.1.1 1G : First Generation (1G) : Analog Cellular

The introduction of cellular systems in the late 1970s and early 1980s represented a quantum leap in mobile communication (especially in capacity and mobility). Semiconductor technology and microprocessors made smaller, lighter weight, and more sophisticated mobile systems a practical reality for many more users. These 1G cellular systems still transmit only analog voice information. The most prominent 1G systems are Advanced Mobile Phone System (AMPS), Nordic Mobile Telephone (NMT), and Total Access Communication System (TACS). With the 1G introduction, the mobile market showed annual growth rates of 30 to 50 percent, rising to nearly 20 million subscribers by 1990. [25] .

2.3.1.2 2G : GSM Data & SMS, WAP

The development of 2G cellular systems was driven by the need to improve transmission quality, system capacity, and coverage. Further advances in semiconductor technology and microwave devices brought digital transmission to mobile communications. Speech transmission still dominates the airways, but the demands for fax, short message, and data transmissions are growing rapidly. Supplementary services such as fraud prevention and encrypting of user data have become standard features that are comparable to those in fixed networks. 2G cellular systems include GSM, Digital AMPS (D-AMPS), code division multiple access (CDMA), and Personal Digital Communication (PDC). Today, multiple 1G and 2G standards are used in worldwide mobile communications. Different standards serve

different applications with different levels of mobility, capability, and service area (paging systems, cordless telephone, wireless local loop, private mobile radio, cellular systems, and mobile satellite systems). Many standards are used only in one country or region, and most are incompatible. GSM is the most successful family of cellular standards (GSM900, GSM–railway [GSM–R], GSM1800, GSM1900, and GSM400), supporting some 500 million of the world’s cellular subscribers with international roaming in approximately 168 countries and 400 networks.

2G to 3G GSM Evolution

Phase 1 of the standardization of GSM900 was completed by the European Telecommunications Standards Institute (ETSI) in 1990 and included all necessary definitions for the GSM network operations. Several tele-services and bearer services have been defined (including data transmission up to 9.6 kbps), but only some very basic supplementary services were offered. As a result, GSM standards were enhanced in Phase 2 (1995) to incorporate a large variety of supplementary services that were comparable to digital fixed network integrated services digital network (ISDN) standards. In 1996, ETSI decided to further enhance GSM in annual Phase 2+ releases that incorporate 3G capabilities.

GSM Phase 2+ releases have introduced important 3G features such as intelligent network (IN) services with customized application for mobile enhanced logic (CAMEL), enhanced speech compression/decompression (CODEC), enhanced full rate (EFR), and adaptive multirate (AMR), high–data rate services and new transmission principles with high-speed circuit-switched data (HSCSD), general packet radio service (GPRS), and enhanced data rates for GSM evolution (EDGE). UMTS is a 3G GSM successor standard that is downward compatible with GSM, using the GSM Phase 2+ enhanced core network.

The GSM Standard

Global System for Mobile Communications (GSM) is the most popular mobile phone system in the world, accounting for 70% of the world’s digital mobile phones. According to a press release by the GSM Association in May 2001, there are more than half a billion GSM mobile phones in use in over 168 countries today. The phenomenal success in mobile telecommunications is due in large to GSM. One of

its key strength is its international roaming capability, giving consumers a seamless service in over 168 countries.

GSM service started in 1991. In the same year, GSM was renamed to Global System for Mobile Communications from Group Spéciale Mobile. Although GSM was initially developed as a European digital communication standard to allow users to use their cellular devices seamlessly across Europe, it soon developed into a standard that would see unprecedented growth globally. Here in North America, the GSM standard is often referred to as PCS 1900 and elsewhere as DCS 1800. The number relates to the operating frequency of the system.

Key features of GSM is:

- International Roaming - single subscriber number worldwide
- Superior speech quality - better than existing analog cellular technology
- High level of security - user's information is safe and secure
- Universal and Inexpensive Mobile handsets
- Digital Convenience - talk time is doubled per battery life and digital networks can handle higher volume of calls at any one time that analog networks
- New services - such as call waiting, call forwarding, Short Message Service (SMS), GSM
- Packet Radio Service (GPRS)
- Digital compatibility - easily interfaces with existing digital networks i.e. Integrated Services Digital Network (ISDN)

Some argue that GSM is not as secure, as publicized. The GSM standard was created in secrecy and all of the algorithms used are not available to the public. Most security analysts believe any system that is not subject to the scrutiny of the world's best minds can't be as secure.

In April 1998, the Smartcard Developer Association (SDA) together with two U.C. Berkeley researchers claimed to have cracked the COMP128 algorithm stored on the SIM. By sending large number of challenges to the authorization module, they were

able to deduce the K_I within several hours. They also discovered that K_C uses only 54 bits of the 64 bits. The remaining 10 bits are replaced by zeros, which makes the cipher key purposefully weaker. They feel this is due to government interference. A weaker ciphering key, could potentially allow governments to monitor conversations.

The SDA did have the SIM in their physical presence when they cracked the algorithm. However they fear “an over the air attack” is not far fetched. Unfortunately, they are unable to confirm their suspicions, as the equipment required to carry out such an attack is illegal here in the US.

The GSM Alliance responded to the incident, stating even if a SIM could be cloned it would serve no purpose, as the GSM network would only allow only one call from any phone number at any one time. GSM networks are also capable of detecting and shutting down duplicate SIM codes found on multiple phones.

In August 1999, an American group of researchers claimed to have cracked the weaker A5/2 algorithm commonly used in Asia, using a single PC within seconds.

In December 1999, two leading Israeli cryptographers claimed to have cracked the strong A5/1 algorithm responsible for encrypting conversations. They admit the version they cracked may not be the exact version used in GSM handsets, as GSM operators are allowed to make small modifications to the GSM algorithms. The researchers used a digital scanner and a high end PC to crack the code. Within two minutes of intercepting a call with a digital scanner, the researchers were able to listen to the conversation. Here in the US, digital scanners are illegal.

The GSM Alliance of North America has claimed that none of its members use the A5/1 algorithm, opting for more recently developed algorithms.

The ISAAC security research group claims it is technologically possible to build a fake base station for roughly \$10,000. This allows a “man-in-the-middle” attack. Essentially, the fake base station can flood the real base station and force a mobile station to connect to it. The base station could then inform the phone to use A5/0 (no encryption) and eavesdrop on the conversation.

An insider attack is another possible scenario. All communication between the Mobile Station and the Base Transceiver Station are encrypted. Beyond that point, all communications and signaling is generally transmitted in plain text within the

provider's network. While a strong defense has been put upfront to deter hackers, the inner core is wide open.

Since the inception of these attacks, the GSM body has been working to patch up the possible security holes. Over the past 12 months, there have been two significant results. Firstly, the compromised COMP128 hash function has been replaced with a patched COMP128-2 hash function. Secondly, a new A5/3 algorithm has also been agreed upon to replace the aging A5/2 algorithm. While they have chosen not to disclose any pertinent information regarding the currently used algorithms, they have taken a step in the right direction with GSM's replacement,

3GPP. They have moved away from their "security by obscurity" ideology with 3GPP (3rd Generation Partnership Project). All the algorithms being used in 3GPP are available to security researchers and scientists.

Despite the recent security breaches, GSM is by far more secure than previous analog cellular systems and continues to be the most secure public wireless standard in the world.

SMS

Short Message Service (SMS) is the transmission of short text messages to and from a mobile phone, fax machine, and/or IP address. Messages must be no longer than 160 alphanumeric characters and contain no images or graphics. SMS is a relatively simple messaging system provided by the mobile phone networks. SMS messages are supported by GSM, TDMA and CDMA based mobile phone networks currently in use. Although services based on SMS have been feasible for many years, the recent mobile phone penetration and large scale adoption of the existing services by users, have made the SMS based services even more attractive to service providers.

Short messages can be sent and received simultaneously with GSM voice, Data and Fax calls. This is possible because whereas voice, Data and Fax calls take over a dedicated radio channel for the duration of the call, short messages travel over and above the radio channel using the signaling path. As such, users of SMS rarely, if ever, get a busy or engaged signal as they do during peak network usage times.

Ways of sending multiple short messages are available. SMS concatenation (stringing several short messages together) and SMS compression (getting more than

160 characters of information within a single short message) have been defined and incorporated in the GSM SMS standards.

To use the Short Message Service, users need the relevant subscriptions and hardware, specifically:

- A subscription to a mobile telephone network that supports SMS
- A mobile phone that supports SMS.
- The use of SMS must be enabled for the user. (automatic access to the SMS is given by some mobile network operators, others charge a monthly subscription and require a specific opt-in to use the service)
- Knowledge of how to send or read a short message using the specific model of mobile phone.
- A destination to send a short message to, or receive a message from. This is usually another mobile phone but may be a fax machine, PC or Internet address.

SMS is one of the few services in consumer history that has grown very fast without corresponding decreases in pricing. Usually- even in the case of voice mobile phones- price reductions in the cost of the phones and phone service have led to increases in usage. Whilst these factors have helped to bring younger people into the mobile market, the price of SMS itself stayed steady because the networks were having trouble handling the volumes of messages being sent and dared not reduce prices.

SMS growth continued its astonishing growth during the year 2000 in Europe, a period of time when the mobile industry was trying to dictate the deployment of WAP. Despite doing nearly nothing else of any benefit, WAP did at least increase the attention that the mobile Internet received as people tried to work out services that would appeal to the mobile phone users. Those companies that survived the WAP debacle started to realize that it was SMS and not WAP that had the addressable audience of users and the clearer business case. Advertising and other services based on SMS started to be trialed as companies realized that people who could use SMS for person to person messaging would also be able to access SMS based commercial messages.[26]

The benefits of SMS to subscribers center around convenience, flexibility, and seamless integration of messaging services and data access. From this perspective, the primary benefit is the ability to use the handset as an extension of the computer. SMS also eliminates the need for separate devices for messaging because services can be integrated into a single wireless device- the mobile terminal. These benefits normally depend on the applications that the service provider offers. [27]

At a minimum, SMS benefits include the following:

- Delivery of notifications and alerts
- Guaranteed message delivery
- Reliable, low-cost communication mechanism for concise information
- Ability to screen messages and return calls in a selective way
- Increased subscriber productivity

More sophisticated functionality provides the following enhanced subscriber benefits:

- Delivery of messages to multiple subscribers at a time
- Ability to receive diverse information
- E-mail generation
- Creation of user groups
- Integration with other data and Internet-based applications

The benefits of SMS to the Service Provider are as follows:

- Ability to increment average revenue per user (due to increased number of calls on wireless and wireline networks by leveraging the notification capabilities of SMS) an alternative to alphanumeric paging services, which may replace or complement an existing paging offer ability to enable wireless data access for corporate users new revenue streams resulting from addition of value-added services such as e-mail, voice mail, fax, and Web-based application integration, reminder service, stock and currency quotes, and airline schedules provision of key administrative services such as advice of charge, over-the-air downloading, and over-the-air service provisioning

- Protection of important network resources (such as voice channels), due to SMS' sparing use of the control and traffic channels notification mechanisms for newer services such as those utilizing wireless application protocol (WAP) all of these benefits are attainable quickly, with modest incremental cost and short payback periods, which make SMS an attractive investment for service providers. [27]

SMS was initially designed to support limited-size messages, mostly notifications and numeric or alphanumeric pages. While these applications are and will continue to be widely used, there are more recent niches that SMS still can exploit.

Short bursts of data are at the heart of many applications that were restricted to the world of data networks with fixed terminals attached to a local-area network (LAN) or wide-area network (WAN). However, many of these applications are better served if data communication capabilities could be added to the mobility of the station. Thus, a waiter who can charge a customer's credit card right at the table, at any time, instead of going to a fixed POS terminal located by the register will be able to help customers in a faster, more convenient way.

Also, the ability to track the location of a moving asset such as a truck or its load is very valuable for both providers and clients. This application, again, just needs to interchange small amounts of information, such as the longitude and latitude at a current time of the day, and perhaps other parameters like temperature or humidity.

This application does not necessarily require the monitored entity to be in movement. The requirements are basically short, bursty data and a location that has digital network coverage. For example, in a neighborhood, it would be faster, easier, and cheaper to drive a truck from the local power company, which interrogates intelligent meters to obtain their current readings and then forwards them via short message to a central data processing center to generate the billing. Similarly, delivery trucks could be alerted of the inventory of a customer running low, when the truck is close to the customer's facilities. The truck driver could place a quick phone call to the customer to offer a short-time replenishment at a low cost for the distributor.

Another family of applications that can use SMS as a data transport mechanism Banking. It is no secret that automated teller machine (ATM) and Internet transactions are less costly than transactions completed at a branch. Internet

transactions are even cheaper than ATM transactions. Therefore, enabling wireless subscribers to check their balances, transfer funds between accounts, pay their bills and credit cards is valuable, not only for the subscriber but also for financial institutions.

Entertainment applications are also good drivers of SMS usage. Examples of these are simple short message exchanges between two parties ("texting") or between multiple participants ("chat"). Also, delivery of information that the subscriber can tailor to his or her lifestyle represents an attractive proposition for wireless users.

Wireless Web browsing allows the users to search for information without the physical restrictions of a PC. College students certainly appreciate not having to go to the computer lab or their dorm to check e-mail or find out what the required book is for the semester that is about to start.

E-mail continues to be by far the most used wireless data application. However, handsets are evolving quickly and are including more and more functionality that supports newer applications at the same time that user friendliness increases. Probably the next big success beyond wireless Web will be Internet shopping and other e-commerce applications such as electronic coupons, advertising, etc.

The potential for applications is enormous, and new needs appear to arise constantly, demanding a solution that may travel over SMS.

WAP

WAP stand for Wireless Application Protocol, and consists of a set of specifications for developing web-like applications that run over wireless networks. The WAP specification is analogous to those used in existing Internet technology but are optimized for the restrictions of small, narrowband devices and limited bandwidth. It is an open, global specification that allows mobile users with wireless devices to easily access and interact with information and services instantly. The development of WAP was lead by a democratic consortium of industry partners known as the WAP Forum.

Wireless Application Protocols (WAP) is designed to address the needs of the wireless industry and deliver a set of protocols to accommodate the devices of the mobile market. Internet standards such as HTML, HTTP, TLS, and TCP are

inefficient over mobile networks, requiring the transfer of large amounts of text-based data. WAP is based on these current Internet standards but have been optimized for the unique constraints of the wireless environment: low bandwidth, high latency, and less connection stability. Standard HTML web content cannot be as effectively displayed on the small screens of mobile phones and pagers. WAP is the streamlined version of the Internet and will enable mobile devices to deal with the functional and bandwidth limitations of cellular networks.

WAP is a global standard and is not controlled by any single company. Ericsson, Nokia, Motorola, and Unwired Planet founded the WAP Forum in 1997 to define an industry-wide specification for developing applications over wireless communications networks.[28]

According to the Gartner Group, Asia-Pacific will see 7.9 million WAP enabled mobile phones sold in 2000, 29.4 million in 2001, 78.8 million in 2002 and 120.9 million in 2003. According to Nokia, by the year 2004, the number of projected Internet enabled handsets will equal the projected number of PCs connected to the Internet at 500 million[26].

Firms that have only begun to make sense of the convoluted business strategies and intricate logistics required by the regular Internet must now contend with the arrival of Wireless Web. Mobile commerce, the next frontier of electronic commerce, is demanding that companies re-think their business models, partnerships and pricing structures in order to accommodate this latest technological advancement and capitalize upon the commercial prospects inherent with the mobile telecommunication industry.

WAP was designed and created to handle higher latencies, unpredictable service availability, unpredictable connection stability, and lower bandwidth of wireless communication. In particular, instability, service availability, and latency problems make it difficult to maintain connection-oriented services like transmission control protocol (TCP). Internet standards such as hypertext markup language (HTML), hypertext transfer protocol (HTTP), transport layer security (TLS) and TCP are inefficient over mobile networks, requiring the transmission of large amounts of text-based data and are not optimized for the intermittent coverage, long latencies and limited bandwidth. HTTP sends its headers and commands in an inefficient text

format instead of compressed binary. Wireless services using these protocols are often slow, costly, and difficult to use. The TLS standard requires multiple messages to be exchanged between the client and server which result in a very slow response for the user. Also, standard HTML content cannot be as effectively displayed on the tiny screens of pocket-sized mobile devices as their desktop monitor counterparts.

A protocol was needed that could efficiently deal with the shortcomings of the cellular networks, and thus WAP was created. Both a communications protocol and an application environment, WAP is a much lighter protocol than TCP/IP, using less overhead to clog up the limited bandwidth or bog down the small processors involved in mobile Internet access. WAP utilizes binary transmission for greater compression of data and is optimized for long latency and low bandwidth. WAP sessions are engineered to cope with intermittent coverage and can operate over a wide variety of wireless transports. WAP also utilizes a new markup language called WML and WMLScript which makes efficient use of small displays and limited navigation capabilities. WAP content is scalable from a five-line text display on cell phones to the full screens on personal digital assistants (PDA).

Advantages :

There are many benefits to having access to a mobile Internet. End users of WAP will benefit from the easy, secure access of the Internet such as messaging, banking, and entertainment through their mobile devices. Users will have significant freedom of choice when selecting a mobile terminal and will be able to receive and request information in a controlled, fast and low-cost environment. Teenagers who have a WAP phone can keep in touch with their friends via ICQ, order movie tickets and items by phone. Business people can use WAP to buy stocks on their way to the airport. They can check news and weather before they buy new clothes for the trip, and log onto the company WAP intranet. They can receive information on the move, get up to date information on weather, stocks, and other developments during commutes. WAP could be utilized to build internal corporate applications like telephone directories.

Most of the already successful interactive services that exist on the Internet can be implemented in a WAP environment as well. Users can take advantage of on-phone shopping, interactive recreational sites and corporate advertising. Also, location-

based services can be used as sophisticated telephony applications. For example, if a user was on travel, a directory service could locate a suitable restaurant or hotel and automatically dial ahead to book. Search engines like Orktopas are currently available on WAP mobile devices to make finding information easier and faster. There is a Chinese and English wireless portal offering 150 interactive services called WAP head that will give Asian users the added convenience of using a language of their choice.

M-Commerce, or mobile commerce, involves mobile shopping and mobile banking. Thailand's MWeb offers an on-line flower delivery service that is gradually adding other services like email, ICQ, news (business, local, international, and sports), lottery results, daily horoscopes, various directories and schedules. Singapore has TheWebWap.com, which offers business to business m-commerce applications that will give their partner companies an on-line WAP presence and allow end-users to make use of their services while on the move, including making on-line reservations and using on-line ticketing services.

Information management offers users a whole suite of tools to organize contacts, files and message data. Applications include address books, calendars, bookmarks and file stores. Future developments include enabling Outlook Express to be exported into the device user profile and eliminate the need for keying in the addresses of current contacts. Group management tools are also available like earth9.com which offers community management tools to enable users to share information with different groups.

The most popular use of the Internet is messaging and email. WAP-mail will allow users to communicate with each other via their mobile devices. ThatWeb.com's UniWapMail has the added convenience of configuring email POP3 servers. NTT DoCoMo's i-Mode currently has over six million subscribers that allow users to send and receive email as well as banking and money transfers.

Many companies have integrated WAP into their business and commercial infrastructure. GeePS.com is combining WAP and Global Positioning System satellite technology to deliver a geographically localized shopping service. The service will enable users to browse and search using their cellular phone and PDS for coupons and discounts offered by stores in their physical vicinity. Andy Goren, CEO

of GeePS.com, says that users are notified by local merchants (within a half-mile radius) with special deals and price comparisons.³ The transaction can be completed using the phone, charging it to the user's credit card. The user then goes to the store and picks up the goods. GeePS.com is tasked to bring brick and mortar retailers the innovative advantages of mobile retail in marketing and advertising that the web had originally brought them.

Disadvantages:

However, there are currently many disadvantages with WAP technology. There are few WAP products that actually exist in the market today to support the technology. WAP phones have little memory capacity and cannot store large amounts of information. This is a definite disadvantage for users who are use to downloading data from the Internet while surfing the web. They will not be able to store the latest mp3 file or retrieve office documents on their mobile devices.

WAP phones are not as advanced as the technology they are supporting. A chief complaint of many users is the frustration and awkwardness of navigating on a WAP phone. Email is much more difficult to compose on a phone than on a desktop PC. There is a need for a better keyboard than the numeric dial pad to write lengthy messages. A possible solution is to implement voice (like Sprint PCS Voice Command) or handwriting recognition software. WAP screens are too small due to their portable nature. Users cannot read the same amount of information as on a desktop PC. The screen quality is not as good and pictures are monochrome. Even though WAP servers can translate Web pages instantly, information can be lost or misrepresented on some devices. The multitude of devices that are present in the marketplace makes it difficult to develop consistency. Different browsers on different mobile devices will interpret WAP pages in various ways.

Despite the fact that WAP can be run on any bearer network, there still remains a need for a protocol specific to wireless communications. The world needs to agree on a bearer standard. In addition, WAP devices are relatively slow. Developers are constantly working on a faster way of sending information. The Global System for Mobile Communications (GSM) network, implemented in most of Europe, is slow at sending information. New network technologies called High Speed Circuit Data

(HSCD) and General Packet Radio Service (GPRS) are aimed at providing a faster connection.

In Australia, WAP is still considered too expensive to be a viable method of service. At an average cost of 20 cents per minute, usage can get expensive. Most WAP users can only view the content prescribed by their carrier and are restricted to viewing only the content provided by their provider's WAP portal. Enclosed services have been described as "walled gardens," where the territory within is closely guarded by carriers.

SMS vs. WAP

SMS is the short messaging service for GSM. It is also present on most other digital cellular networks and tends to operate in a similar fashion on each network. SMS enables 2-way short messages to be sent between GSM subscribers. Using gateways, it is also possible to interchange messages with other systems such as Internet email, the web etc. So, SMS is essentially a messaging transport service to enable reliable 2-way messaging.

WAP on the other hand is a "protocol set" aboard which various services can be delivered. Like any protocol, it states how devices can be made compatible ("speak the same language") in order to exchange information. Since SMS is a means for information to be transported, two devices could use SMS to exchange WAP-compliant data.

As well as being a transport service, SMS also has a protocol. However, as mentioned earlier, the SMS protocol is really only concerned with reliable 2-way messaging and so it is restricted to basic functionality. In protocol terms, this means a very basic command set such as "Send Message" and "Receive Message". Clearly for anything more sophisticated, this protocol is very limited. However, there's nothing to stop another protocol being added on top with more commands that just get sent using the Send and Receive of SMS. This is what WAP does.

So why does WAP do this? Well, to use the mobile phone to converse with any information-delivery system (such as the web or a database), the method of delivery needs to be tailored to the limitations of the phone - mainly the small text-only display, and the restrictive keyboard and navigation keys. So a part of WAP is

concerned with sensible data formatting and navigation appropriate to these limitations. However, sending data over mobile air interfaces poses problems with delays and slow links. These can be overcome to an extent by optimizing the way in which the protocol is mapped to the interface (such as the SMS carrier or an ordinary GSM data call). Another part of WAP is concerned with efficient protocol transport.

So is SMS still needed after WAP? The answer is yes. Firstly there are many applications that simply do not need WAP. The simple send and receive primitives of SMS are sufficient. Also, there is often no need, or no context, to maintain an ongoing (connected) communications session over SMS and so SMS tends to get used in a connectionless mode, like sending a letter or an email - whereby immediate, or even any, response is not required (though it may be desirable at times).

Many SMS messages are alerts of one kind or another, used to notify the recipient of an event. These types of messages usually require follow-on action other than sending a reply using SMS. In these circumstances, SMS is sufficient and there is no need to move to WAP.

Secondly, WAP is not widely available yet and there are millions of phones that can handle SMS but not WAP. These will stay in circulation for some time.

WAP is particularly useful for interactive services on the handset. Interactive services can be realized using native SMS, but this is not as elegant as WAP. Using WAP, the user can be prompted for information and guided along the interactivity path, whereas while using only SMS, the user has to remember how to respond with any preset commands.

So, do we need SMS or WAP or both? The answer is both are needed and they have different uses and applications. SMS is particularly good for pushing out information to mobile phone users. In particular, Xsonic InTouch monitors a variety of data sources within the Microsoft Exchange messaging server and pushes out alerts, such as "new email from...", "appointment at..." etc. Xsonic DataNow also generates alerts from any data changes that occur within an SQL Server database.

Alerts can be followed up by a variety of actions. These may include SMS replies of one form or another. Additionally, SMS can be used to pull data from a database.

This feature gets used in Xsonic InTouch to pull contact details from a user's personal contacts folder in the Exchange database. In this way a mobile worker could get the fax number of a customer, their address, home phone number etc. For many of these types of applications, the quick alert or prompt/pull operations of SMS are ideal. Indeed, an advantage of SMS is that it is quick.

The advantage of WAP is that it enables greater interactivity with the data source. This would be useful, for example in any operation that is multi-paged in nature (such as navigating through a hierarchy). Traversing an email Inbox is one such application. With Xsonic InTouch, a WAP phone could be used to receive SMS alerts (e.g. calendar reminders, email notification etc.) and the user could then elect to respond with short SMS commands and get a quick reply, or they could elect to connect to the server via a secure remote access point and navigate through the various Exchange folders.

SMS and WAP are different entities and are often complimentary. A well-designed application would exploit the essential characteristics of SMS and WAP to suit the end-user requirements. For fast alert or quick-shot pull systems, SMS is a good solution. For any communications requiring ongoing interaction with a hierarchical data source, WAP is a good solution. Sometimes, both solutions can be used to get the best of both worlds.

2.3.1.3 2G+: HSCD & USSD, GPRS

High Speed Circuit Switched Data (HSCSD)

High Speed Circuit Switched Data (HSCSD) is an enhancement of data services ("Circuit Switched Data - CSD) of all current GSM networks. It allows you to access nonvoice services at 3 times faster, which means subscribers are able to send and receive data from their portable computers at a speed of up to 28.8 kbps; this is currently being upgraded in many networks to rates of and up to 43.2 kbps. The HSCSD solution enables higher rates by using multiple channels, allowing subscribers to enjoy faster rates for their Internet, e-mail, calendar and file transfer services.

HSCSD allows you to access your company LAN, send and receive e-mails, access the Internet whilst on the move. HSCSD is currently available to 90 millions

subscribers across 25 countries around the world and with the implementation of International Roaming agreements between all HSCSD Operators life on the move just got easier.

HSCSD is offered to subscribers using either voice terminals that support the feature, or a special PCMCIA portable computer card, with a built in GSM phone that turns notebook computers and other portable devices into a complete high-speed mobile office with the ability to make voice calls hands free, as well as data transfer. The HSCSD service is particularly valuable for customers who wish to access the Internet, or their office Intranet, access their mail, or access files stored elsewhere. The service allows a subscriber who is out of office, or who travels abroad in one of the countries in which HSCSD roaming is available, to connect to a local ISP, or directly to one's office, using the cellular device rather than a fixed line, benefiting from significant improvements in rates of transfer. The service offered through HSCSD enabled GSM cellular handsets directly, in addition to the PC compatible device.

The basic GSM data services [29] have been in the market for about 6 years. However, they have not reached wide scale usage. Some of the basic reasons are low throughput and dependability of GSM data transmission. ETSI [30] has planned a technology path to higher throughput and more dependable services. High Speed Circuit Switched Data (HSCSD) [31, 32] and 14400 bps channel coding (144CC) [33] were the first steps in the path. General Packet Radio Services (GPRS) [34] is entering the market, and Universal Mobile Telecommunications Services (UMTS) succeed them within next 2-3 years. HSCSD offers higher transfer rates by combining two or more time slots. It implements a flexible time slot allocation scheme. The allocation of time slots depends on the following factors: end user's subscription, air capacity, and network load.

HSCSD uses an Automatic Link Adaptation scheme (ALA) for the best channel coding at each occasion. GPRS enhances GSM data services to a packet switched data transmission. GPRS has also a flexible time slot allocation scheme and ALA. In the first phase, GPRS uses CS-1 (9.05 kbps line rate) and CS-2 (13.4 kbps line rate) channel codings. [32]

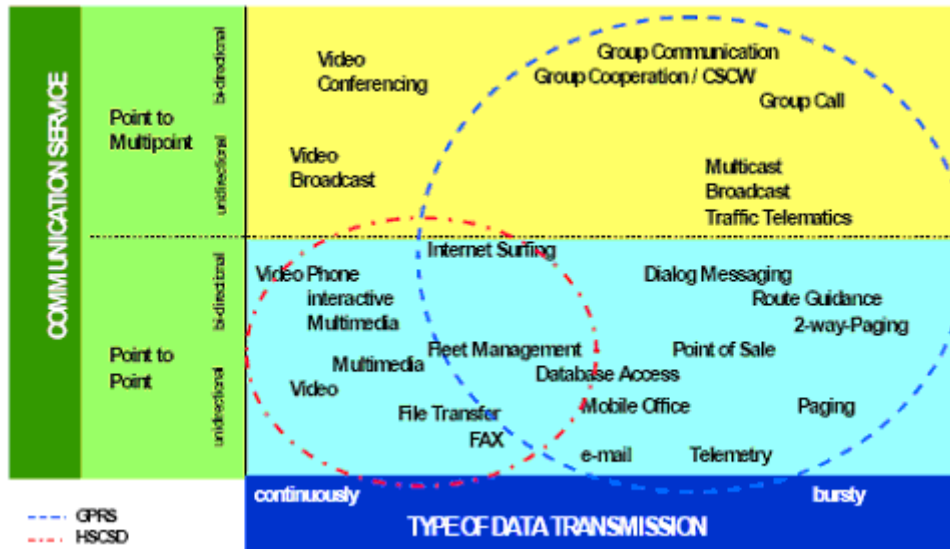


Figure 3: GSM 2+ Data services and their applications

HSCSD consists of two separate technologies: multislot capability and modified channel coding scheme. The former provides the usage of several parallel time slots per user thus increasing the user data rate respectively. The first phase of HSCSD specifications allows the usage of 4+4 time slots, but in practice, the mobile equipment manufacturers implement more limited versions of that. At the beginning of HSCSD services, the maximum number of time slots is mostly limited to 1+3 and 2+2 (Fig. 4). The specifications define asymmetric traffic in such a way, that the amount of time slots in uplink direction cannot exceed the number of time slots in downlink direction.

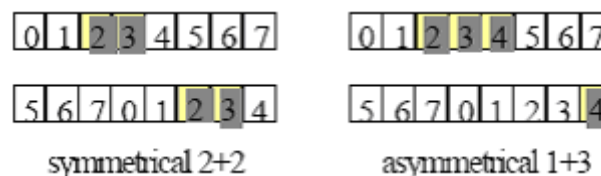


Figure 4:Example of symmetric and asymmetric HSCSD multi slot-scheme

The 144CC scheme provides a 14.4 kbps line rate instead of the original 9.6 kbps line rate. In order to achieve higher line rates there is a more efficient puncturing method used, which on the other hand decreases the radio interface error correction

performance. This means, that 144CC cannot be used, when there are a lot of noise and interference affecting the quality of the radio signal. The specifications define upgrading and downgrading of air interface resources. It means that the amount of parallel time slots can vary between one and the maximum defined value. Up- and downgrading may occur when the signal level, interference level or capacity varies during a connection. The system can also use ALA, which means that the data rate can be 14.4 kbps or 9.6 kbps for an individual time slot depending on the radio path conditions. Both up and downgrading of the resources and ALA can happen during a data transfer. Even though, the specifications allow the up- and downgrading and ALA, the combinations might be limited depending on the network and mobile terminal capabilities.

In the first phase, the maximum data rate of HSCSD is limited to 64.0 kbps due to the A-interface. Depending on the connection type and the infrastructure capabilities of the network, the maximum user rate can be 38.4 kbps using ISDN V.110 protocol, and 57.6 kbps using ISDN V.120 protocol.

The air interface user rate in the original GSM data transmission is limited to 9.6 kbps with the 12 kbps air interface rate. The HSCSD allows higher air interface user rates to be used for transparent and non-transparent data services.

HSCSD is a feature enabling the co-allocation of multiple full rate traffic channels (TCH/F) into a HSCSD configuration. The aim of HSCSD is to provide a mixture of services with different air interface user rates by a single physical layer structure. The available capacity of a HSCSD configuration is several times the capacity of a TCH/F, leading to a significant enhancement in the air interface data transfer rate.

With HSCSD higher transmission rates than the current 9.6 kbit/s can be achieved, see GSM 02.34 [32]. The GSM HSCSD feature is capable of supporting up to 64 kbit/s user rate. This is achieved by two mechanisms:

- Channel combining: Combining up to 8 channels within the same call.
- Channel coding: A-channel coding of 14.4 kbit/s instead of 9.6 kbit/s is introduced.

As a result, HSCSD is a circuit switched service targeted at applications which require higher bandwidth and continuous data streams, making it an ideal solution for

applications which require a constant delay (e.g. video). It is only applicable for Point to Point communication. For bursty and bulky data transmission the General Packet Radio Service (GPRS) was designed. The following figure shows the different target applications of these services.

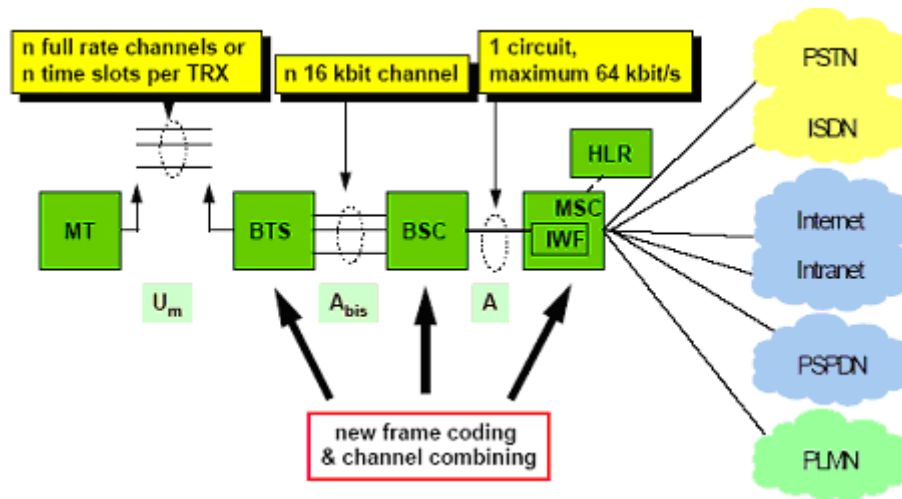


Figure 5: HSCSD / 14.4 kbps /Channel Combining System impacts

In general, in good radio signal quality environment, both HSCSD and GPRS provided significantly better throughput and response time than the basic GSM data service. The throughput and round-trip time in stationary connections were stable. However, in moving connections they may change a lot; for example, the throughput changed between 23.2 kbps and 2.4 kbps and response time changed between 2.3 sec and 26.8 sec. One of the reasons to the high vTelconce was the behavior of TCP. TCP could not cope properly with the characteristics of HSCSD and GPRS data transmission, thus causing performance slow down by doing a lot of unnecessary retransmissions. The problems with TCP are discussed, for example, in [32]. IETF has started to address these problems [33].

HSCSD provided better performance than GPRS does. GPRS had higher vTelconce in performance than HSCSD. The high vTelconce needs to be addressed when developing nomadic applications over GPRS. The reliability in stationary connections is adequate. But the reliability in moving connections – a disconnection every 11th-12th minute (HSCSD) or long pauses in data transfer (GPRS) – may

create problems, for example, in long web browsing sessions or in long file transfers. Therefore, the reliability of moving connections may create problems, if a distributed application cannot cope properly disconnections or long pauses.

Unstructured Supplementary Service Data (USSD)

Unstructured Supplementary Services Data (USSD) is a means of transmitting information or instructions over a GSM network. USSD has some similarities with SMS since both use the GSM network's signaling path. Unlike SMS, USSD is not a store and forward service and is session-oriented such that when a user accesses a USSD service, a session is established and the radio connection stays open until the user, application, or time out releases it. This has more in common with Data than SMS.

USSD text messages can be up to 182 characters in length. USSD is defined within the GSM standard in the documents GSM 02.90 (USSD Stage 1) and GSM 03.90 (USSD Stage 2). In USSD Stage 1, the interactions are initiated by the mobile phone. In USSD Stage 2, the application can also initiate USSD-based transactions. Turnaround response times for interactive applications are shorter for USSD than SMS because of the session-based feature of USSD, and because it is NOT a store and forward service. According to Nokia, USSD can be up to seven times faster than SMS to carry out the same two-way transaction.

Users do not need to access any particular phone menu to access services with USSD- they can enter the Unstructured Supplementary Services Data (USSD) command direct from the initial mobile phone screen. Creating and sending a USSD message is as easy as making a call. Indeed, most handsets allow a subscriber to store USSD strings under quick dial keys .Creating a USSD message can be easier than creating a mobile originating short message.

Because messages can be exchanged with the Home Location Register (HLR), subscribers can send USSD messages back to your network even when they are roaming on other networks. Providing the visited network supports the necessary functionality, USSD provides a way of delivering value added services to your subscribers seamlessly -even when they are roaming and as such, USSD provides an alternative to CAMEL.

Unstructured Supplementary Services Data (USSD) works on all existing GSM mobile phones. Both SIM Application Toolkit and the Wireless Application Protocol support USSD.

USSD Stage 2 has been incorporated into the GSM standard. Whereas USSD was previously a one way bearer useful for administrative purposes such as service access, Stage 2 is more advanced and interactive. By sending in a USSD2 command, the user can receive an information services menu. As such, USSD Stage 2 provides WAP-like features on EXISTING phones.

On the down side, Unstructured Supplementary Services Data (USSD) strings are typically complicated for the user to remember, involving the use of the "*" and "#" characters to denote the start and finish of the USSD string. However, Unstructured Supplementary Services Data (USSD) strings for regularly used services can be stored in the phonebook, reducing the need to remember and reenter them. There is considerable flexibility both in terms of the length and content of the message.

- USSD makes use of all the digits plus the * and # characters.
- Formatting of USSD messages (the parameters) can be summarized as follows:
 - An asterisk is used to separate each of the parameters
 - A service code of 2 or 3 digits is entered
 - Supplementary information can then be entered. This may be of vTelcoble length.
 - As an example, a Personal Identification Number may be used as a measure of security.
 - The # key terminates a request.
 - A valid USSD message request may, therefore, look something like this:
*14*123*123456789#

No other mechanism has thus far been specified in the draft third generation Universal Mobile Telephone System (UMTS) standards to carry out the functions such as Home Location Register (HLR) interaction that USSD facilitates. As such,

Unstructured Supplementary Services Data (USSD) is likely to still find applications in the third generation world [34].

USSD, which is most suitable for enabling dialogue-based applications, is used to send text messages between the user and some mobile applications. It provides an ideal mechanism for the mobile terminal to trigger or access mobile services such as callback, interactive messaging, information enquiry services, banking services, customer service and mobile chat. At the end of this paper, there is a project sampled in order to use USSD in an mobile banking application.

Attributes of USSD

USSD commands initiated in a foreign network are routed back to the HLR (Home Location Register) of the mobile's home network. This allows home services to continue to work just as well when subscribers are roaming. The turnaround response times for interactive applications are shorter for USSD as compared to SMS. This is because USSD provides a session-oriented service while SMS uses a store-and-forward, transaction-oriented technology.

Users do not need to access any particular phone menu to request USSD services. They can enter the USSD command directly from the mobile phone screen. USSD works on most existing GSM mobile phones which both SIM Application Toolkit and the Wireless Application Protocol supports [35].

USSD Service Flow

Typically, a user requests a service by entering a short code (e.g. *121* 676#) on his mobile phone. The format of the short code follows USSD standard but its content is specific to each service.

The short code contains the service code (e.g. 121) and optional service-related information (e.g. 352). This code is passed across the mobile network to the USSD gateway and routed to the application. The application sends the response back to the subscriber through the USSD Gateway within the same USSD session. For USSD Phase II, the session can consist of an unlimited sequence of messages between the subscriber and the application. In addition, a USSD session can also be initiated by the application.

USSD Server

USSD Gateway is designed with high-performance platform, fault-resilient SS7 signaling unit and well-established database software. It integrates high quality products in the market that makes it a high performance, robust and reliable system.

It has complex logic to support multiple applications within a single platform. It is able to scale from several SS7 signaling links to tenths of them. It provides the wide-deployed SMPP (Simple Messaging Peer-Peer) interface for applications to enable their services. This allows new services to get deployed rapidly and encourages existing messaging applications to leverage on USSD technology.

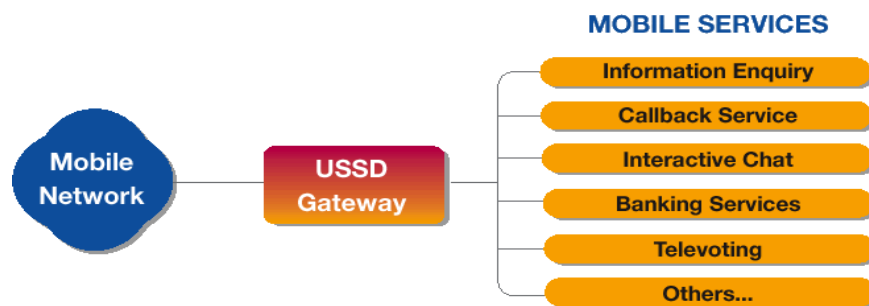


Figure 6: Sequence of Operations

USSD provides an ideal way for subscribers to request changes to their class of service or to request that enhanced services are performed. To achieve this, the sequence of operations is as follows:

- A Subscriber sends a mobile originating USSD message
- The USSD message is routed to the subscriber's HLR in accordance with the GSM recommendations
- The HLR forwards the USSD message to the USSD Gateway
- The USSD Gateway communicates the message to external applications using
- TCP/IP - a protocol which is more convenient for integration with commercial computing platforms.

- The external system interprets the message and, where appropriate, performs the value added service indicated by the content of the message.
- Within a time-out period, the external system acknowledges successful receipt of the message to the mobile via the USSD Gateway. The external system can later asynchronously send further information to the mobile as a Short Message via an SMS.

In summary the key benefits of USSD are:

- Easy to use. Keying a digit string can be easier for a user than formatting a short message. Strings may be stored under abbreviated dial keys on the handset.
- USSD messages are very flexible in both length and content.
- Almost all handsets can send USSD messages (* and # need to be available) whereas many existing handsets do not support MO SM. In many markets this means the population addressable with these services are hugely increased.
- USSD is faster than MO-SMS.
- Roaming supported. Because messages are exchanged with your HLR, services are still available when roaming.
- Service access codes and service names may be downloaded to the handset using Over the Air Programming. This makes it even easier for the user to get started.

There are a number of differences between MO-SMS and USSD. USSD is not store and forward, and does not offer retries, so it is simpler and faster than SMS. Clearly, the service does not offer guaranteed delivery, but any failures are reported back to the originator. Against this, USSD should achieve many times the speed of SMS due to its simplicity and much-reduced reliance on non-volatile storage. In addition, it offers a simple TCP/IP interface to external applications, which need know nothing of the SS7 network. Routing to applications is achieved via a simple service code which is contained in the USSD message. The interpretation of the Service Code is achieved by configuration of the USSD Gateway and by the actions of the External

Application to which the Service Code relates. The External Applications can be on any machine reachable by a TCP/IP network.

General Packet Radio Service (GPRS)

Wireless communications lets people live and work in ways never before possible. With over two hundred million cellular subscribers worldwide, users have overwhelmingly embraced the concept of having a telephone that is always with them. And now business users also want a data connection with the office wherever they go, so that they can have access to e-mail, the Internet, their files, faxes and other data wherever and whenever it is needed, giving them a competitive advantage and more flexible lifestyles. A number of wireless data services are available today, but none are as exciting as a forthcoming data service for GSM networks called General Packet Radio Service (GPRS).

GPRS refers to a high-speed packet data technology, which is expected to be deployed in the next two years. It is expected to profoundly alter and improve the end-user experience of mobile data computing, by making it possible and cost-effective to remain constantly connected, as well as to send and receive data at much higher speeds than today. Its main innovations are that it is packet based, that it will increase data transmission speeds from the current 9.6 Kbps to over 100 Kbps, and that it will extend the Internet connection all the way to the mobile PC -- the user will no longer need to dial up a separate ISP. GPRS will complement rather than replace the current data services available through today's GSM digital cellular networks, such as circuit-switched data and Short Message Service. It will also provide the type of data capabilities planned for "third generation" cellular networks, but years ahead of them.

GPRS, which is first acquired by Telsim, is already rare around the world. Telsim, which is the 3rd telecom operator serves this service in the world, has 10 million dollar investment for the GPRS. [36]

The most important aspects of GPRS are that it allows data transmission speeds to over 100 Kbps, that it is packet based, and that it supports the world's leading Internet communications protocols, Internet Protocol (IP) and X. 25.

The fact that GPRS will operate at much higher speeds than current networks should provide a huge advantage from a software perspective. Today, wireless middleware is often required to allow slow speed mobile clients to work with fast networks for applications such as e-mail, databases, groupware or Internet access. With GPRS, wireless middleware will often be unnecessary, and thus it should be easier to deploy wireless solutions than ever before.

Whereas today's wireless applications tend to be text oriented, the high throughput offered by GPRS will finally make multimedia content, including graphics, voice and video practical. Imagine participating in a videoconference while waiting for your flight at the airport, something completely out of the question with today's data networks.

Why is packet data technology important? Because packet provides a seamless and immediate connection from a mobile PC to the Internet or corporate intranet allowing all existing Internet applications such as e-mail and Web browsing to operate smoothly without even needing to dial into an Internet service provider. The advantage of a packet-based approach is that GPRS only uses the medium, in this case the precious radio link, for the duration of time that data is being sent or received. This means that multiple users can share the same radio channel very efficiently. In contrast, with current circuit-switched connections, users have dedicated connections during their entire call, whether or not they are sending data.

Many applications have idle periods during a session. With packet data, users will only pay for the amount of data they actually communicate, and not the idle time. In fact, with GPRS, users could be "virtually" connected for hours at a time and only incur modest connect charges. While packet-based communications works well with all types of communications applications, it is especially well suited for frequent transmission of small amounts of data, what some call short and burst, such as "real time" e-mail and dispatch. But packet is equally well suited for large batch operations, and other applications involving large file transfers.

GPRS supports the widely used Internet Protocol (IP) as well as the X.25 protocol. IP support is becoming increasingly important as companies are now looking to the Internet as a way for their remote workers to access corporate intranets. The IP protocol is ubiquitous and familiar, but what is X.25, and why is support for it

important? X.25 defines a set of communications protocols that prior to the Internet constituted the basis of the world's largest packet data networks. These X.25 networks are still widely used, especially in Europe, and so wireless access to these networks will benefit many organizations. But what does this really mean? Quite simply it means that any existing IP or X.25 application will now be able to operate over a GSM cellular connection. You can think of cellular networks with GPRS service as wireless extensions of the Internet and existing X.25 networks, as shown in Figure 7.

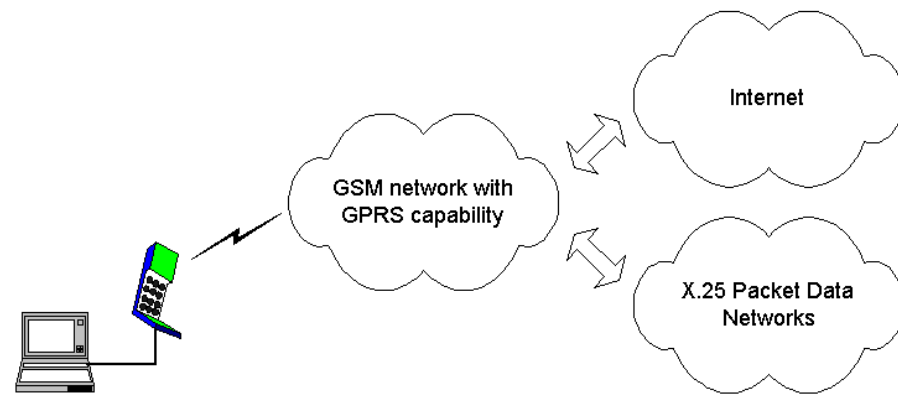


Figure 7: GPRS as an extension of other packet networks.

We now look more closely at how the user takes advantage of GPRS. The packet nature of GPRS, which makes a GPRS connection similar in many ways to a local area network (LAN) connection. Just as with a LAN connection, once a GPRS mobile station registers with the network, it is ready to send and receive packets. A user with a laptop computer could be working on a document without even thinking about being connected, and then automatically receive new e-mail. The user could decide to continue working on their document, then half an hour later read the e-mail message and reply to it. All this time the user has had a network connection and not once had to dial in, as he or she must today with circuit-switched connections. Furthermore, GPRS allows for simultaneous voice and data communication, so the user can still receive incoming calls or make outgoing calls while in the midst of a data session. Since there is almost no delay before sending data, GPRS is ideally suited for applications such as extended communications sessions, e-mail

communications, database queries, dispatch, and stock updates to name just a few. In addition, the high throughput of GPRS will remove many of the obstacles from the use of multimedia, graphical web-based applications. For example, mobile users will be able to easily use graphically intensive web-based map application to get directions while traveling. Furthermore, with almost no transmission delay and high throughput, it will be more practical to use enterprise applications such as SAP* wirelessly and remotely.

Because GPRS supports standard networking protocols, configuring computers to work with GPRS will be very straightforward. In the case of IP communications, you can use existing TCP/IP protocol stacks, such as the stack that comes with Windows 95 or Windows 98, Windows CE and Windows NT. TCP/IP stacks are readily available for most other platforms as well. With all the developments in the handheld computer area, you can expect a multitude of hardware platforms to take advantage of GPRS:

- Laptops or handheld computers connected to GPRS-capable cellphones or external modems
- Laptops or handhelds with GPRS-capable PC Card modems
- Smart phones that have full screen capability
- Cell phones employing micro browsers using the Wireless Application Protocol
- Dedicated equipment with integrated GPRS capability, e.g. mobile credit-card swipers

GPRS coincides with another important technology development: the replacement of a cable connection to a cellphone by a short radio link. Intel, Ericsson, Nokia, IBM, Toshiba and others are already working on such wireless connections in an initiative called "Bluetooth".

GPRS is also complementary with an important industry trend associated with remote access: the transition from dial-up remote access to Internet-based remote access.

Traditionally companies have provided remote access for their workers using dial-up modem connections into corporate modem pools. But as companies have established high speed connections to the Internet, and as remote workers have an increasing number of options for connecting to the Internet, companies are now looking to the Internet as a way for their remote workers to access corporate intranets. This is especially effective because most communications applications today work over IP networks -- including many originally designed for modem dial-up connections. It can be highly cost effective to use the Internet instead of making long distance phone calls, and in the case of international connections, much more reliable. But this Internet-based technique does raise an issue of privacy from hackers. A new technology is emerging which addresses privacy and authentication concerns, referred to as a virtual private network (VPN).

A VPN is a method of having private communications across public networks. It adds additional software at each end of the connection -- in our case the mobile computer and the corporate network. This software establishes what are called "tunnels". Within this tunnel, information is encrypted and additional information is added to each packet to prevent tampering. Various standards are available or being finalized to define interoperability between VPN products, including the Point to Point Tunneling Protocol (PPTP), Layer Two Tunneling Protocol (L2TP), SOCKS and IPsec (Secure IP). A wide range of companies already offer VPN solutions today, including router vendors, network software providers, firewall suppliers and companies specializing in this area. Since most VPN solutions are quite flexible in their feature set, corporate IT can choose the level and type of protection desired, such as 56-bit encryption or 128 bit encryption.

Almost all VPN technologies operate independently of the communications link, meaning the same VPN technology will work with a dial-up modem connection, Ethernet connections, ISDN connections and most importantly for us, wireless connections. See Figure 8.

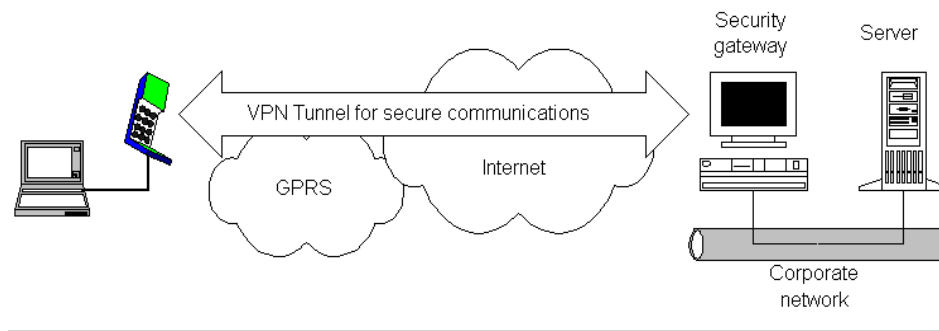


Figure 8: Tunneling with VPN technology

Companies using VPNs will be able to smoothly migrate from existing wireless technologies to GPRS. Today their users can make circuit-switched connections to an Internet service provider, and then establish a VPN connection. Once GPRS becomes available, the Internet connection will extend to the mobile computer and the user will no longer need to dial a separate ISP. The net result is wireless connectivity that works hand in hand with VPN technologies to let remote workers easily access corporate resources and to stay in touch with their work teams.

An interesting aspect of GPRS is how it achieves its high speeds to over 100 kbps when circuit-switched data today is limited to 9600 or 14.4 kbps. GPRS uses the same radio channel as voice calls, a channel that is 200 kHz wide. This radio channel carries a raw digital radio stream of 271 kbps that for voice calls is divided into 8 separate data streams, each carrying about 34 kbps. After protocol and error correction overhead, 13 kbps is left for each voice connection or about 14 kbps for data. Circuit-switched data today uses one voice channel. GPRS can combine up to 8 of these channels, and since each of these can deliver up to 14 kbps of data throughput, the net result is that users will be able to enjoy rates over 100 Kbps. But not all eight-voice channels have to be used. In fact, the most economical phones will be ones that are limited to 56 kbps. The GPRS standard defines a mechanism by which a mobile station can request the amount of bandwidth it desires at the time it establishes a data session.

2.3.1.4 3G : Universal Mobile Telecommunication System (UMTS)

Mobile data communications is evolving quickly because of Internet, Intranet, Laptops, PDAs and increased requirements of workforce mobility. 3G UMTS will be

the commercial convergence of fixed line telephony, mobile, Internet and computer technology. New technologies are required to deliver high-speed location and mobile terminal specific content to users. The emergence of new technologies thus provides an opportunity for a similar boom what the computer industry had in 1980s, and Internet and wireless voice had in 1990s.

The main characteristics of 3G systems, known collectively as IMT–2000, are a single family of compatible standards that have the following characteristics:

- Used worldwide
- Used for all mobile applications
- Support both packet-switched (PS) and circuit-switched (CS) data transmission
- Offer high data rates up to 2 Mbps (depending on mobility/velocity)
- Offer high spectrum efficiency

IMT–2000 does the International Telecommunications Union (ITU) define a set of requirement? As previously mentioned, IMT stands for International Mobile Telecommunications, and “2000” represents both the scheduled year for initial trial systems and the frequency range of 2000 MHz (WARC’92: 1885–2025 MHz and 2110–2200 MHz). All 3G standards have been developed by regional standards developing organizations (SDOs). In total, proposals for 17 different IMT–2000 standards were submitted by regional SDOs to ITU in 1998—11 proposals for terrestrial systems and 6 for mobile satellite systems (MSSs). Evaluation of the proposals was completed at the end of 1998, and negotiations to build a consensus among differing views were completed in mid 1999. All 17 proposals have been accepted by ITU as IMT–2000 standards. The specification for the Radio Transmission Technology (RTT) was released at the end of 1999. The main IMT–2000 standardization effort was to create a new air interface that would increase frequency usage efficiency. The WCDMA air interface was selected for paired frequency bands (FDD operation) and TDCDMA (TDD operation) for unpaired spectrum. 3G CDMA2000 standard was created to support IS-95 evolution.[37]

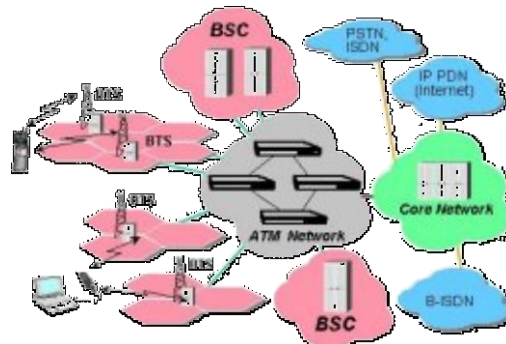


Figure 9: UMTS Network

The UMTS transport network is required to handle high data traffic. A number of factors were considered when selecting a transport protocol: bandwidth efficiency, quality of service, standardisation stability, speech delay sensitivity and the permitted maximum number of concurrent users. In the UMTS network, ATM (Asynchronous Transfer Mode) is defined for the connection between

UTRAN and the core network and may also be used within the core network. In addition to the IMT-2000 frame many new standards will be integrated as part of the next generation mobile systems. Bluetooth and other close range communication protocols and several different operating systems will be used in mobiles. Internet will come to mobiles with WAP, i-mode and XML protocols. 3G development has helped to start the standardization and development of large family of technologies. Bell Laboratories invented the cellular concept, and the first commercial analog systems introduced in the early 1980s were designed purely for voice communications. The advanced mobile phone system (AMPS), the first (pre-operational) system, was introduced to Chicago in 1979. The North European countries devised the Nordic Mobile Telephone (NMT) system for Scandinavian coverage in 1981. It started in Sweden and quickly expanded to Norway, Denmark, and Finland. The UK introduced its first cellular system in 1985 using an analog standard called TACS (total access communications system), based on the AMPS system.

Thus, users were largely confined to the systems their phones were designed for, roaming between systems was virtually impossible, and there was no agreed-upon

path for getting the various first-generation systems onto a common platform. GSM grew out of the first-generation cellular system's limitations and the desire of European countries to develop a common cellular telephony standard. In June 1982, the first meeting for the second-generation system was held in Vienna and a new standardization body called Groupe Spéciale Mobile (GSM) was born. The first meeting was held in Stockholm in December 1982, with 31 people from 11 countries attending. Its goals were to help develop high-volume, mass-market products that would reduce the cost of cellular services, make roaming between countries easy, and introduce integrated services such as data, fax, and short messages, in addition to encrypted digital speech and advanced fraud protection.

GSM is not just a radio interface but a specification for a complete network, which was to be launched in various stages, with phase 1 covering basic service and phase 2, enhanced services. The term GSM was retained as the commercial trademark for the 900-MHz system.

Although there is no tight, unambiguous definition for the third-generation mobile system, the goal of system operators, manufacturers, and governments is to provide high functionality with seamless global roaming. Third-generation systems should support high-speed data and multimedia applications of up to 144 kb/s while moving any distance, and up to 2 Mb/s wireless access in a local area. The third-generation mobile system is designed to give users consistent voice, data, graphical, multimedia, and video-based information service, regardless of their location on the network (cordless, cellular, satellite, fixed/wire line, and so on).

Note that UMTS will support data-rates of much more than 2 Mb/s in wireline service. Whereas the previous mobile systems were separate from wireline telephony systems, Europe wants UMTS to integrate wireline and mobile systems.

In a nutshell, UMTS can be split into two main areas of standards-setting: core network and wireless access. To date, most of the work has concentrated on the wireless part; UMTS will be introduced in Europe by the year 2002 in the form of the UMTS air interface.

The new wireless wideband systems will offer both real time (for example, for speech) and non-real-time modes (say, for e-mail) using common transport

mechanisms. The future transport mechanism will provide an efficient transport mechanism for message, file, and stream-type data defined as:

Message packet data: time-delay tolerant, but requiring a low bit-error rate (BER). This is generally a fixed-length single packet, for handshake-type operations, and for signaling packets and mobile features like SMS (short message service).

File packet data: for multiple packets, also time-delay tolerant but requiring the data to arrive perfectly intact (whereas with speech, for example, some bits can be lost). The content varies in length and could include downloading Internet pages, transferring files, e-mail, and so on.

Stream connection-oriented data: separable into two subgroups. "Speech" and "video phone" applications are stream-delay intolerant but more flexible in their BER demands. Video broadcasts have some stream-delay tolerance, such as where the terminal may store the data, but small time delays are acceptable. Each type of application requires different characteristics of its communications link. UMTS will provide the appropriate access mechanisms for each application, obtain maximum network efficiency, and save customers money.

Higher bandwidths, asymmetrical connections, and dynamic bandwidth allocation will offer better system flexibility for both network operators and customers. The network operator will make more efficient use of network resources like the radio spectrum. Customers may save money by being able to pay per data packet. Current services generally force them to pay for a set bandwidth that is wasteful because data is usually "bursty" and the connection is rarely used to its maximum. Employing the Internet as an example, the user sets up a data connection to a service provider (normally a two-way symmetrical link equating to a two-way 9.6-kb/s link in GSM). When a page is initially accessed, the user requires a large data dump. The application is time tolerant, and packets of data arrive at different times. The traffic is mainly one way (downloaded).

Once the information is received, the customer normally reads the page and keeps the communications link alive. UMTS will maintain a virtual link, by means of signaling (as opposed to the data) channel, so that once the data has been downloaded, the customer pays nothing more until the next information request. In addition, UMTS will potentially offer an asymmetrical two-way link allowing large

data-dumps to the customer while retaining only a small link in the opposite direction. During the time the user is reading the downloaded page, network resources can be reallocated to other users.

The third-generation mobile system is customer focused: its aim is to provide seamless services regardless of terminal type, network, or access method. As part of the service ethos, the virtual home environment (VHE) is another new customer option. VHE let customers retain and personalize their services anywhere--and use them at any time in both wireless and wired environments. Third-generation systems also allow users to determine the quality of the voice or video call, and pay accordingly.

Users will have specific services--voicemail, fax, and perhaps some video services--which they will resort to regularly. They may also set up an easy way to access the services, possibly using a Web browser and short codes to telephone friends. If the customer roams to a different country and hence to a different network operator, UMTS will ensure that the specific services are not only available, but that his or her preferences are retained. The preferences may include how goods purchased over the Internet are paid for and how services react when the bandwidth is decreased. With videoconferencing, a customer may opt to retain high-quality speech and to lose the video when the bandwidth or link quality declines.

Employing the same mobile videoconferencing example, a user may set up a videoconference with a colleague while in the office. The office will provide high-bandwidth access (possibly a private cable with much more than 2 Mb/s or a wireless picocell with up to 2 Mb/s). The network/application will choose a video-coding standard (in software) that provides both high-quality pictures and high-quality sound.

The security functions of UMTS are based on what was implemented in GSM. Some of the security functions have been added and some existing have been improved. Encryption algorithm is stronger and included in base station (NODE-B) to radio network controller (RNC) interface, the application of authentication algorithms is stricter and subscriber confidentiality is tighter.

The main security elements that are from GSM:

- Authentication of subscribers
- Subscriber identity confidentially
- Subscriber Identity Module (SIM) to be removable from terminal hardware
- Radio interface encryption

Additional UMTS security features:

- Security against using false base stations with mutual authentication
- Encryption extended from air interface only to include Node-B to RNC connection
- Security data in the network will be protected in data storages and while transmitting ciphering keys and authentication data in the system.
- Mechanism for upgrading security features.

Mobile data communications is evolving quickly because of Internet, Intranet, Laptops, PDAs and increased requirements of workforce mobility. 3G UMTS will be the commercial convergence of fixed line telephony, mobile, Internet and computer technology. New technologies are required to deliver high-speed location and mobile terminal specific content to users. The emergence of new technologies thus provides an opportunity for a similar boom what the computer industry had in 1980s, and Internet and wireless voice had in 1990s.

2.4 Mobile Security

2.4.1 Introduction

The requirements of information security have undergone three major changes in the last decades. The first major change was the introduction of the computer. The need for protecting files and information became evident. Collection of tools designed to protect data and to avoid hacker attacks has the generic name *computer security*. The second major change was the introduction of distributed systems, networks and communication facilities for data communication. *Network security* measures are needed to protect data during transmission. The third change is the current, rapid

development of wireless networks and mobile communications. *Mobile security* is therefore of high priority today.

The telecommunications industry has been one of the fastest growing industries in the 1990s. The number of mobile phone users and the amount of data transferred wirelessly has increased drastically. Moreover, the demand for mobile data services such as banking, shopping, and e-mail has been growing constantly. However, a part of these services, e.g. banking, requires strict security and a publicly accepted way of authentication. This arises the need for a tailored security and authentication system for mobile transactions.

2.4.2 Problems Arising From Mobility

In comparison with wired media, the wireless communications requires more comprehensive solutions for network security, since radio waves are broadcast to the surrounding environment. There is no means to limit the people or devices that can listen to the transmissions. Therefore the signals need to be encrypted before transmission and decrypted at the other end of the wireless communications channel. However, as the mobile terminals gain access to the Internet or other external networks, the

requirement for other kind of secrecy than protection of communications channel emerges. While wireless media is protected by its own secrecy protocol, there is no such an automatic protection in the Internet. However, some of the secrecy requirements in the Internet are solved with Secure Socket Layer (SSL) that provides a protected connection between two parties. There is also a similar solution in the transport layer of the Wireless Application Protocol (WAP) called Wireless Transport Layer Security (WTLS). These two standards provide often secrecy at some level, but they lack, e.g. efficient authentication tools.

There are also numerous other factors weakening the protection in mobile communications. First, some terminals have low calculation capacity. A part of cryptographic algorithms require extensive calculation and therefore their suitability for mobile secrecy may be limited. Second, the quality of the connection to the mobile terminal may be poor and the integrity of the transactions has to be guaranteed. Third, there will be several different kinds of terminals and single users will have usually many of them (e.g. mobile phone, PDA, laptop, home computer,

and work computer). Authentication should be possible to carry out in the same way regardless of the terminal the user is using.

Mobile networks have properties that imply different security solutions for wired and wireless networks. These are (Rysavy, 1998)[38]:

- □ They use the same networking protocols but use specialized physical and data link protocols
- □ They connect to existing networks via access points which provide a bridging function
- □ They let you stay connected when roaming from one coverage area to another
- □ They have unique security considerations
- □ They have specific interoperability requirements
- □ They require different hardware
- □ They offer performance that differs from wired LANs

Mobile communications is rapidly evolving. An overview of security aspects of needed systems, standards and protocols is given in (Hansen, 2000) (A Comparison of Security in HomeRF versus IEEE802.11b, 2001) (Wireless LAN Security, 2001)[39].

2.4.3 Secure Network Principles

Network security is one of the key aspects of the present telecommunications industry. A potential failure in the security may result in an outflow of crucial secret information to competitors. As in most high technology sectors, the protection of a firm's proprietary technology is a central factor in order to attain a sustainable competitive advantage (cf. Porter, 1985). There are five main areas of network security, which are considered in security systems: 1) *secrecy*, 2) *integrity*, 3) *availability*, 4) *authentication*, and 5) *non-repudiation* (Tanenbaum 1996).

By secrecy we require that only the person to whom it is addressed can read the message. The sender typically encrypts messages, and the receiver has a key that can open (decrypt) the message.

Integrity states that the receiver should always be able to verify whether the message contains real information. Moreover, it should be verified that the message has not been changed during the transmission.

Availability refers to the fact that the sender should always be able to send his message to the receiver if he intends to do so. Authentication in turn refers to the ability of identifying the sender of the message.

Non-repudiation is closely intertwined with the requirement of authentication. It states that the sender cannot claim that he has not been the sender of a message. Instead, the message must have a mechanism, such as time stamps and digital signatures that reveal the sender unambiguously.

2.4.4 Mobile Systems of Second Generation

Digital 2G systems, such as GSM, PDC, IS-136 TDMA and IS-95 CDMA, use cryptographic methods for authentication and confidentiality. GSM (General System for Mobile communications) is a standard for digital cellular communications. This standard implements security features, which ensure **(Kesarev, 1997)[40]**: 1) physical security, 2) data security, 3) user authentication, and 4) user anonymity. Slow frequency hopping and modulation techniques enhance the physical security. Information sent between a mobile station and the network is encrypted. Further, monitoring signals of the radio interface requires specialized equipment not freely available.

GSM security is based on a shared secret key K_i and on a unique number, the International Mobile Subscriber Identity (IMSI). Both are on the user's Subscriber Identity Module (SIM) and in the Authentication Centre (AuC) of the operator. A signal response number (SRES) is calculated by AuC from K_i , IMSI and from a random number challenge (RAND). SRES and RAND are placed in the Home Location Register (HLR). A mobile terminal is authenticated if its calculated SRES is equal to the stored one. The authentication algorithm is called A3, which is a secret algorithm **(Harte, Levine and Livingston, 1999) [41]**.

The encryption algorithm - A5 - is a secret, symmetric stream cipher using a 64-bit key K_c . The key is handled by three Linear Shift Feedback registers (LSFRs). Key K_c used in algorithm A5 is generated by another secret algorithm, A8. This key-

generating algorithm uses RAND and Ki as input (Harte, Levine and Livingston, 1999). Anonymity is achieved by using a Temporary Mobile Subscriber Identity (TMSI). This identity is agreed upon after authentication and key generation through an A5-encrypted channel.

2.4.5 Mobile Systems of 2.5 Generation

GPRS (General Packet Radio Service) is announced to be a mobile system of 2.5 generation. GPRS is rather similar to GSM using the same radio access network in packet mode. Packet handling nodes have to be added. Such nodes are SGSN (Serving GPRS Support Node) and GGSN (Gateway GPRS Node). Other nodes like HLR (Home Location Register) and AuC (Authentication Center) can be reused with minor modifications.

Internet and Intranet access of mobile and portable devices will be major GPRS applications. GPRS will also be a major carrier of WAP (Wireless Application Protocol) applications. Most GPRS terminals will probably also support GSM. The theoretical data rate is more than 100 kbps but most operators will offer data rates between 20 and 40 kbps (SIG, 2001) [42].

Mainly GPRS offers the same security mechanisms as GSM. The same authentication algorithms and also the SIM-card can be used. The cryptographic key is situated in SGSN in contrast to GSM where the key is placed in the base station (SIG, 2001).

Special cryptographic algorithms are used and the length of the used keys is 64 bits. Localization of a mobile station and the use of temporary user identities is supported. Security in the backbone net and between operators is not standardized.

2.4.6 Mobile Systems of Third Generation

Evolving 3G systems, such as UMTS and CDMA2000, will rely on IP-networks, i.e. open networks, which do not separate signaling from user data. This may allow malicious users to gain access to data and/or network resources. An Internet like security architecture will be adopted by the 3G systems. Third generation systems will support roaming with second-generation systems. The compatibility between 2G

and 3G systems will probably give a lower security level (**Steele, Lee and Gold, 2001**) [43].

A smart card will be an obligatory personal security module and it is called USIM. Like in GSM, algorithms for authentication and key generation will be on this card.

New security features are added to take account of changes in network architecture and to secure new services offered by 3G. Compared to GSM two major security developments are included (**Knight, 2000**): [44]

The cryptography used will be strengthened with the introduction of 128-bit keys. A 128-bit cipher key CK and a 128-bit integrity key IK will be established. Information is encrypted between the mobile station and Radio Network Controller node. Encryption relies on the Kasumi algorithm (**SIG, 2001**).

Mutual authentication will be introduced using cryptographic keys to establish the identity of both user and base station over a connection. Authentication for users passing between different networks will also be protected using a public key cryptographic system. The algorithms are based on Rijndael (**SIG, 2001**).

Compared to GSM important signaling is also encrypted. A cryptographic sum check is used in both directions. Also signaling between networks will get standardized security solutions. Confidentiality and integrity will be supported.

3 M-COMMERCE SERVICES

3.1 Introduction

Mobile voice is quickly becoming a commodity and mobile operators are increasingly looking for ways to reduce the loss of subscribers to cheaper competitors and at the same time open up new revenue streams. Offering mobile electronic commerce services is a way of achieving both of these goals. The enabling technology is rapidly advancing and operators must act now to become central player in this lucrative market.

In this section we will look at the m-commerce market and to produce promising business models and service scenarios. As a second aspect the current and emerging technologies behind m-commerce will be investigated and the elements considered in an advanced m-commerce service platform will be looked at. This contribution will give an overview of some of the experiences gained at the m-commerce market, and presents some results achieved so far.

M-commerce is difficult to define. Many people hearing the term for the first time assume it is merely a transfer of e-commerce to a mobile device. However while some of the existing e-commerce services could be used on mobile devices, many of them are simply not suitable due to screen size, lack of keyboard or low bandwidth. Trying to sell m-commerce to consumers as "E-commerce On Your Mobile" could very well lead to the same consumer disillusionment that occurred when WAP was sold as "The Internet On Your Mobile". To allow the creation of a set of mobile commerce services, which users will adopt and from which extra revenue can be generated, the unique attributes of mobiles (portability, secure interaction capability, personalization, access to mobile accounts, etc.) must be leveraged against the disadvantages mentioned.

3.2 M-Commerce Services

It is investigated that more than 25 potential service scenarios falling into 7 categories of services. (Further service scenarios can be taken from various studies and reports) These have been analyzed and categorized and possible obstacles to their deployment have been identified. With these scenarios an insight was gained of what functionality and technologies are needed for the underlying platform and the considerations that have to be made for the business case. Certain key factors were identified that influence the evolution of the services and have to be considered for their assessment:

Stages of the purchase process that are addressed (i.e. information, selection, payment / commitment to a payment, fulfillment, after sales service)

- Security
- Advantage of mobile operator towards competitors
- Regulatory Issues
- User acceptance/market maturity issues
- Network Technology availability
- Building blocks available for m-services
- Suitability of service for mobile devices in terms of design and functionality (selection interface, bandwidth and memory issues)

The services identified within this scope may be classified according to the user type, market segment, and technical aspects. The classification of the service scenarios according to the user types (private and business users) and according to the market segment (B2C, C2C or B2B) is presented below.

3.2.1 Private Users

This includes B2C services where a transaction takes place between customers and a professional offerer (service provider, information provider or a shop), and C2C services where the user transacts with other users.

B2C: The majority of service scenarios deal with the exchange of products, services or information between businesses and consumers. B2C service scenarios can be further divided into categories corresponding to different m-commerce areas. In the following three of these categories are described:

- **Financial Services.** The user experiences financial and payment related services via mobile device. Examples like Mobile Banking services provide public information (e.g. exchange rates, interest rates), as well as private information (checking account and credit card balances, transferring funds, and paying invoices). Additionally Mobile Broker-age services offer buying and selling stock, managing portfolio etc.
- **Mobile Information Provisioning.** This includes services like Mobile Alert, Maps and Routing Direction, and Location Based Information. The information comes mainly either from users' private data like calendar or address book, or content made available by a mobile shop or a Content Service Provider.
- **Mobile Advertising.** The possibilities for mobile marketing are extended and a variety of new advertising methods can be envisaged, replacing gradually advertising messages sent via SMS. Marketing campaigns like a digital coupons service can certainly be successful towards consumers, as the gathering and storage of digital coupons is easier than traditional paper based coupons.
- **Mobile Entertainment, Mobile Shopping, and Local Services** are other important categories of B2C services.

C2C: This category deals with services that provide the necessary infrastructure to enable transactions and exchange of information between two or more private users. Examples of such services are mobile auction services like real-time m-Auctions and services that allow users to share content.

3.2.2 Business

Among the business service scenarios, a distinction has been made between scenarios that allow B2C scenarios to be adapted to a business context, and pure business scenarios that need integration into the internal system of the company.

B2C services for business purposes permit business users to use a B2C service for business purposes.

B2B: The business services considered here provide a mobile channel to a business infrastructure and mainly target a process integration and optimization by allowing employees or business partners to access data or processes of the business infrastructure. Such services often need a strong integration with the Supply Chain Management systems, CRM systems or other systems of the company's internal infrastructure.

3.2.3 Technical Aspects

The technical aspects categorization of m-commerce services deal with the following:

- Terminal constraints that concern small screen size, limited storage capacity, low processing power and lack of keypad reduce usability, security, navigation as well as functionality. Improvement to all these features will boost m-commerce services.
- Connection type can be a deciding factor for mobile commerce services because it determines the bandwidth and important security issues, and makes the distinction between local and global centralized services
- Secure infrastructure: technologies like Public Key Infrastructure and SET protocol are important for the development of special security infrastructure.
- Value added infrastructure: e.g. Location Identifier and Voice Recognition servers

3.3 Examples For M-Commerce Services

The four m-commerce services mentioned in the following paragraphs and pictures were chosen for the deduction of business models. These particular four were picked from the multitude of services which succeed on the market and create revenue for mobile operators were considered particularly high. They both met the user's expectations and gave the operator the opportunity to take a leading role in the service.

3.3.1 Location Based Services

Location based services are an excellent example of how service providers can make use of the inherent properties of mobile devices. The user is always carrying his device with him and the mobile operator can localize the device. He does not even have to know where he is but will get information about his environment by connecting to his service provider. The provider localizes him with the help of the mobile operator and sends him information that is not only based on the user's location but also on his personal preferences. The possibility of user localization is also used in intelligent advertising to allow merchants to address customers near to their shops or restaurants without the customer having explicitly asked for offers. The following figure gives an example of how a location based service could work.

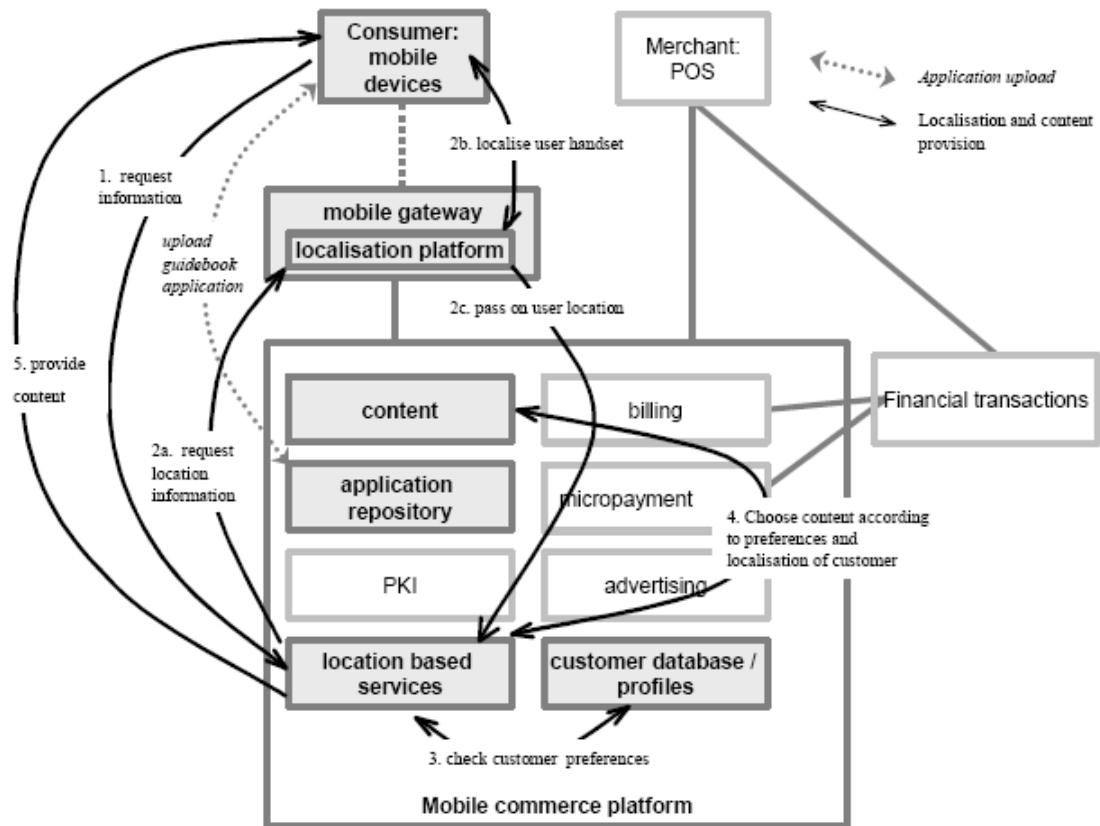


Figure 14: Example of a location based service

3.3.2 Mobile payment

Payment is an important issue when it comes to adoption and acceptance of services by the customers. With the mobile payment service specified in the figure the customer can turn his mobile phone into a payment device and use it to pay for items and services at a real or virtual point of sale subsequently. For payment of a chosen item he gets a purchase order by the merchant, signs it with his private key and sends it back. The payment is safe, easy and quick. As the payment is offline and the service provider is only involved in the clearing process the transaction costs can be kept low. The user can even stay anonymous if he wants to. Thus the mobile payment is the perfect enabling service for many other m-commerce services that involve the transfer of small amounts of money (e.g. downloading of ring tones and music files or access to mobile content).

Figure 15 shows how a mobile payment service could be implemented.

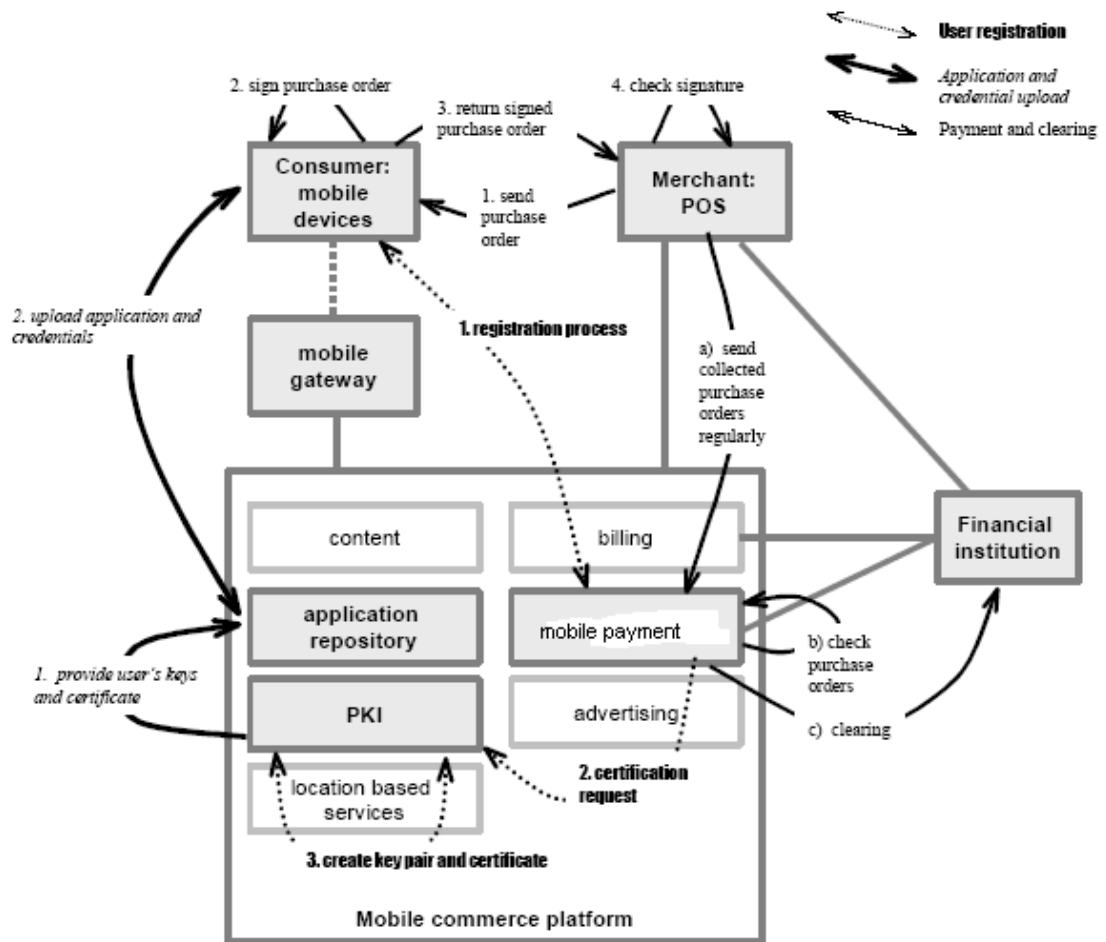


Figure 15: Example of a mobile payment service

3.3.3 Gambling

The gambling and betting services, such as lotto, instant games and sports betting, are very popular in the real world. Offering corresponding services in a mobile environment shows potential to become a quick and convenient way for a mobile operator to get revenue out of the B2C markets. Mobile users can place their bets using text-based technologies like SMS or WAP or play games. Gambling is an excellent example of how an entertainment service could attract customers by offering rich, though often mainly text based contest with a degree of user interactivity and a real-time user experience. Mobile gambling appeals to people's natural desire to win and offers them a pleasant activity they can access anytime and anywhere. The operator should realize the market pull for mobile betting and gambling and seize the chance to develop those promising services into business models.

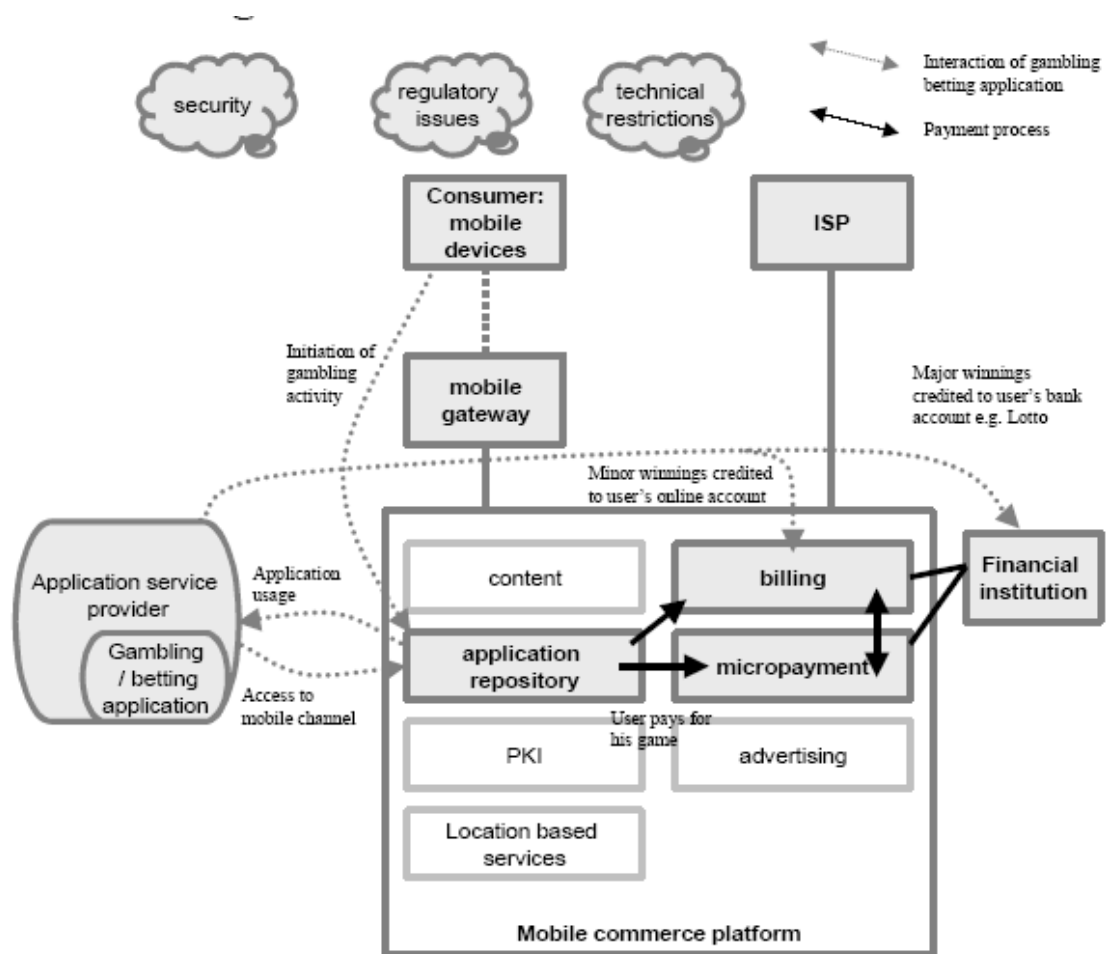


Figure 16: Example of a mobile gambling service

3.3.4 Intelligent Advertising

The basic idea of an intelligent advertising service is that customers receive advertisements (e.g. via SMS or MMS) from merchants on his mobile phone that are adapted to their personal preferences and location based.

The service requires a close collaboration between service providers: The Mobile Advertisement Service Provider takes care of the preparation of the ad, while the owner of the customer database has to define the target group it will be sent to. The mobile operator's task is selecting those of his customers that fit to the target group and providing location information. The customer has to give the permission in advance to receive ads from the mobile operator. If he is interested in an offer, he purchases the product or service directly by connecting to the Mobile Advertisement Service Provider via the mobile operator. The main advantage of the service is that

merchants can be sure to reach the right person by knowing the user profile so they are likely to be willing to pay for it. Of course users will only accept the service if they can be sure that they will not be spammed by unwanted ads.

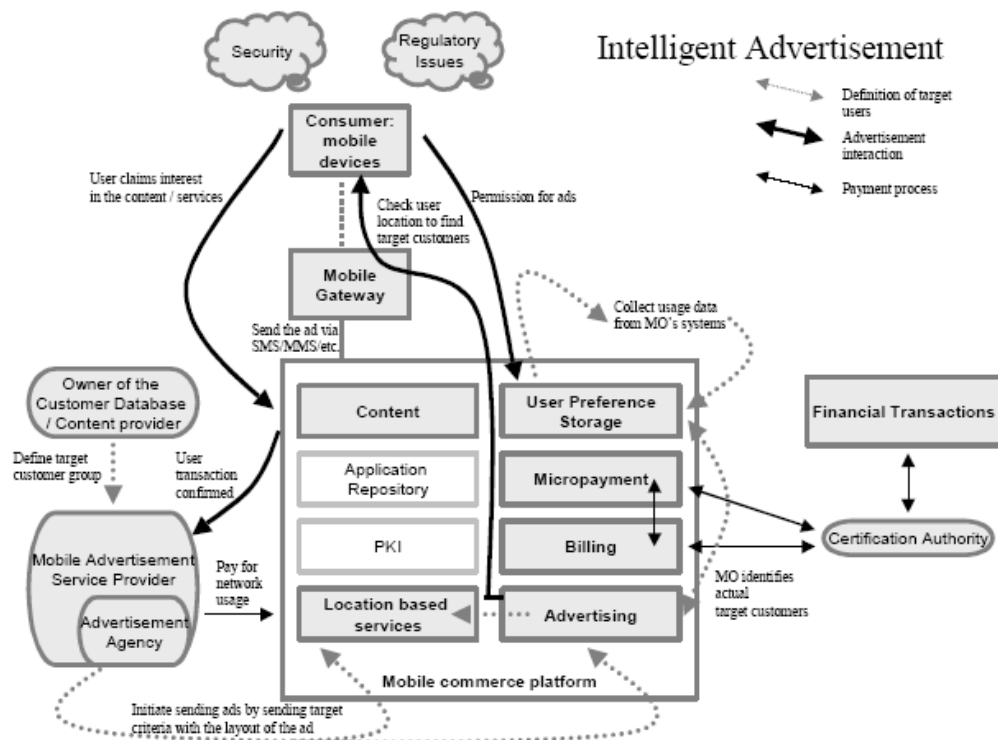


Figure 17: Example of an intelligent advertising service

3.4 Mobile Payment

3.4.1 Understanding The Background Of Mobile Payments

We define a payment as a transaction of a monetary value from one party to another party. This can be done through one or many intermediaries, such as a bank or a card company. By enabling new technologies, especially wireless, we expect to see more possibilities to initiate a payment transaction. The objective is to improve payment systems to approach a more frictionless process.

Traditionally, in the real world, the most popular modes of payments are cash, cheques, debit cards and credit cards. With the possibilities created by the Internet, a new generation of payments appeared, such as electronic payments, digital payments and virtual payments. Now, with the growing penetration of the mobile phone and

the development of m-commerce, the mobile payment will become an uncontested mode for paying goods.

A logical evolution occurred in the monetary value transaction environment due to the progress of technology. In fact, at the beginning, payments were mostly conducted on a face-to-face basis (cash-, paper-, card-based). As technology progressed, remote transactions gained in popularity with the development of data wired networks (credit cards, e-payments).

The current trend is now to implement wireless systems that can handle remote as well as face-to-face mechanisms with a single device.

3.4.2 Micropayments And Macro payments

An important strategic issue for mobile payment system suppliers is to choose the type of payment dimension they want to focus on. For example, micro payments generally represent a payment which is below 10 Euros and is usually supported by cash or debit cards. Merchants are reluctant to accept credit card transactions for small amounts because of transaction fees. Consequently, mobile payments could be an attractive substitute for this type of transaction, especially since most current mobile purchases are news alerts, logos and ring tones.

However, most companies promoting micro payments failed because the margins on small value payments are notoriously low, and sufficient economies of scale are extremely difficult to attain [45]. On the other hand, macro payments, which are thus logically every payment above 10 Euros, represent a real challenge for mobile payments. They need stronger security mechanisms because of the large amount of money involved and the greater possibility of fraud.

A survey from SpeedFacts shows a very surprising fact: the mobile phone is the preferred payment method between 12.5 and 50 Euros [46].

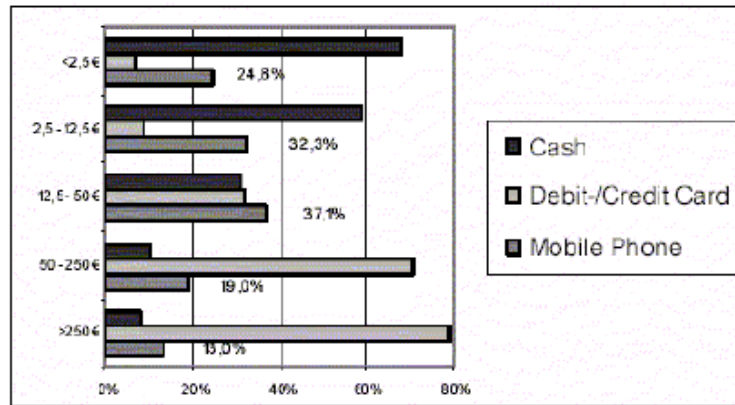


Figure 18: Preferred Payment Method of Internet Users if Away

3.4.3 The Exploration Of Mobile Payments

In spite of the differences between the various mobile payment systems, most of them are similarly structured [47]. As we can see on Figure 24, in most cases a customer needs a payment intermediary.

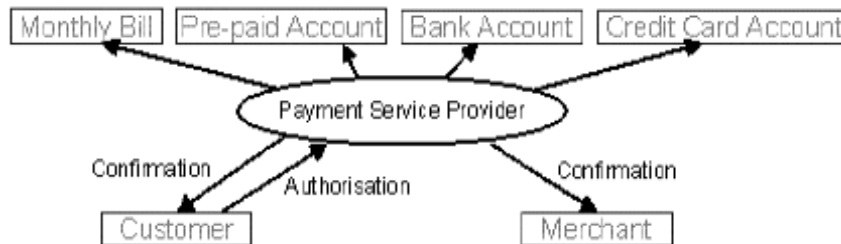


Figure 19: The Structure of Mobile Payments

To be successful, we suggest that a mobile payment solution should be able to handle most of the dimensions presented in Table 3. In general, consumers will be more predisposed to subscribe to a very flexible and universal system compared to another that would not offer the same number of possibilities. Furthermore, the payment solution must always be available since consumers want to pay anytime and anywhere.

There are different reasons why a mobile phone has the potential to become a payment device in the future. The number of users of mobile phones is already

considerable, and mobile payments can be made in all types of payment transactions, such as manned (any merchant), unmanned (vending machines, parking meters...) POS and e-commerce via a mobile phone [48].

The benefits of using a wireless device to pay are narrowly linked to the convenience of using an easy, real-time, cashless and frictionless payment system. Consumers expect mobile payments to be easy-to-use, fast, personalized, secure and universal. The challenge for a wireless device is that it should be able to conduct any transaction, anytime and anywhere.

However, mobile payments also bring many problems to solve. One of the most crucial issues is the price that a mobile payment will be charged. More than ever, consumers are reluctant to pay more without having an added value service; arguments like convenience and security will probably not be attractive enough. Moreover, Dahlberg argues that, from the businesses' perspective, SMS and value added services are considered expensive, and operator's and banks' transaction fees irritate some consumers [49]. Hence, service providers have to find the right revenue model if they want the mobile users and merchants to adopt their new mobile application. Otherwise, there is no chance that the mobile payment solution will succeed. Technology suppliers also have the mission to design mobile devices that are easy-to-use, fast and reliable in a payment context. Without a convenient device, the consumer will not make any effort. A very popular m-commerce example is the book ordered in 40 minutes using a mobile phone!

To summarize the various factors that can lead a mobile payment system to success, Watson proposes a list of four features that can be applied to mobile payments [50]:

- *Ubiquitous* (anywhere, anytime)
- *Universal* (universally usable)
- *Unique* (customized)
- *Unison* (synchronized)

Important actors like Visa and Acceture who co-published a white paper on the U-commerce share this vision. They introduce universal commerce as an environment where buyers and sellers will literally be able to conduct commerce anytime, anywhere and any way they like [51]. Moreover, they predict that this new

environment will provide more choice, more convenience, and more control over how business will be done with one another.

However, this still implies the continued existence of traditional payment means such as cash, checks, debit and credit cards. For them, several global phenomena, such as the pervasiveness of technology, the growth of wireless and increasing bandwidth and connectivity are market drivers that accelerate as technology goes forward.

In order to determine the success of a payment system, de Clercq proposes some commercial, juridical and technological requirements [51].

Table 3: **Some Requirements for the Success of a M-Payment System**

Commercial Requirements	Juridical Requirements	Technical Requirements
Universality	Digital signature	Network technologies
Instant connectivity	Current legislation on payment systems	Service technologies
Personalization		M-commerce terminals
Convenience		M-commerce security mechanisms
Expenses		
Protection of the privacy		
Security		

3.4.3.1 Technologies Enabling Mobile Payments

The intention of this section is not to detail all the technologies involved in mobile payments. Nevertheless, we categorize the different technologies. Therefore, we introduce a mobile payment framework (Figure 25) inspired from a m-business application framework designed by [52].

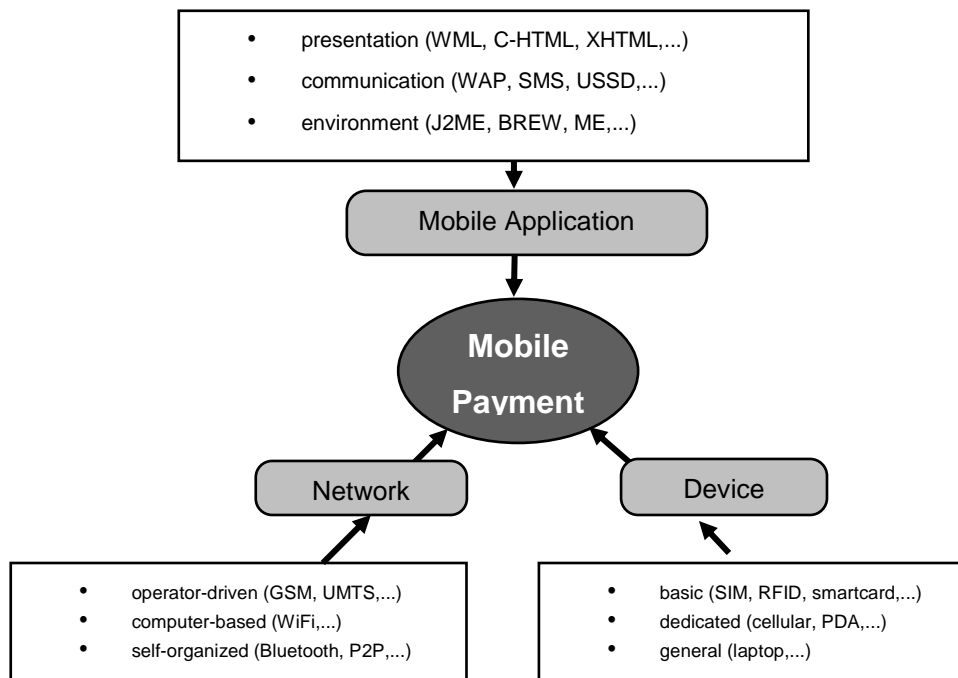


Figure 20 : Mobile Payment Framework

We propose three dimensions to classify the different technologies in mobile payments. First, «Network» gathers the technologies used in a wireless network infrastructure. Then, «Device» represents the user wireless infrastructure. Finally, «mobile application» describes the technologies used mostly by mobile application developers, mobile application service providers and content providers.

3.4.3.2 Security In Mobile Payments

Security in mobile payments is certainly one of the most important problems that providers encounter. In fact, there is no guarantee of total security while sending sensitive information over an open network like the Internet. So far, the two main card association initiatives are Visa 3-D Secure Specification and MasterCard SPA [53]. However, there are some major consortia or forums (e.g. MeT Initiative, Mobey Forum, Mobile Payments Forum and Paycircle) trying to gain the clout that mobile payment players believe they need to create a workable m-payment system [54]. They all want to develop standards to provide secure mobile transactions. Security is also a very critical factor in enabling consumers to trust mobile payments.

A mobile payment solution should respond to the five classic security criteria such as:

- Authentication
- Availability
- Confidentiality
- Data Integrity
- Non-repudiation

Since financial services like payments can be subject to fraudulent activities, they require well-secured infrastructure. The potential flaws are that someone can eavesdrop on the communication and that a third-party impersonifies the provider. Therefore, authentication and confidentiality should be implemented in the solution to prevent these flaws. Security can be hardware or software-based. On the client side, there are at least four [55] or five [56] potential designs for mobile phones to accommodate secure mobile payment (see Table 4).

Table 4 : Four Possible Handset Designs to Enable Secure Mobile Payments

Multi-application chip card	SIM and WIM (Wireless Identification Module) combined in a single chip card
Dual-SIM phone	Both the SIM and WIM have their own slot inside the mobile phone
External WIM card reader	An external card reader can be connected to the handset
Dual-slot phone	The mobile phone has a built-in smart card reader. Consumers insert their existing debit or credit card into the smart-card reader-slot and type in a four digit PIN, issued by their bank, in order to authenticate purchases
Payment software built into phone	The functionality of the WIM would be inside the phone memory.

To prevent the fact that consumers have to replace their mobile phones, most current system use a SMS or USSD-based solution for authentication and payment confirmation mechanisms. This is the case for most newcomers and intermediaries

mobile payment schemes. The only way for mobile payment mass adoption would be if the client device would not cost too much.

As discussed above, security can also be implemented in the network infrastructure. In order to fulfill the security requirements at the network layer, some researchers designed a functional model of a mobile commerce terminal [57].

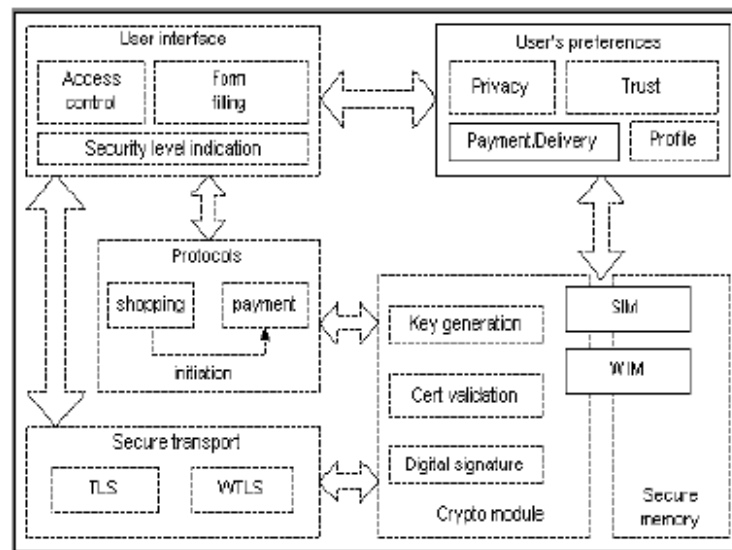


Figure 21 : Functional Model of a Mobile Terminal Designed for Mobile Commerce Applications

This functional model describes the sophisticated mechanisms and protocols. The designers stress that in addition to transport layer security protocols (e.g., TLS and WTLS), it is important to provide an access to basic cryptographic system from the application layer. Nowadays, the cryptographic algorithms used are SHA-1 and 3DES. Moreover, in the future,

AES might be implemented in the terminal. Public Key Infrastructure (PKI) can also be used in the mobile context. However, the PKI will have to support efficient mechanisms for certificate management (e.g., issuing, distributing, validating and revocating the certificate)[57].

Security is probably one factor of success in mobile payment transactions. For now, the biggest challenge is agreeing on few technology standards that would be able to rally most actors on the payment market. Salvi and Sahai propose that subscribers should be able to specify different levels of security for different amounts [1].

Therefore, they suggest four increasing levels of security which can be applied to the payment service (Table 5).

Table 5 : Security Levels

Level 0	No PIN is required. For making micro payments.
Level 1	PIN to authorize payments.
Level 2	PIN + digital certificate signed by a third party on behalf.
Level 3	Digital certificate stored in the mobile and protected by PIN.

3.4.4 The Mobile Payment Arena

The first step in this section of the actual mobile payment market is to identify the main actors, which participate actively or passively. There is a difference made between an actor, which can be involved directly in a mobile payment transaction (Players) and another actor, which has also an importance, but not in the real-time processing (Rulers). Each actor brings its own contribution to enable the mobile payment mechanisms.

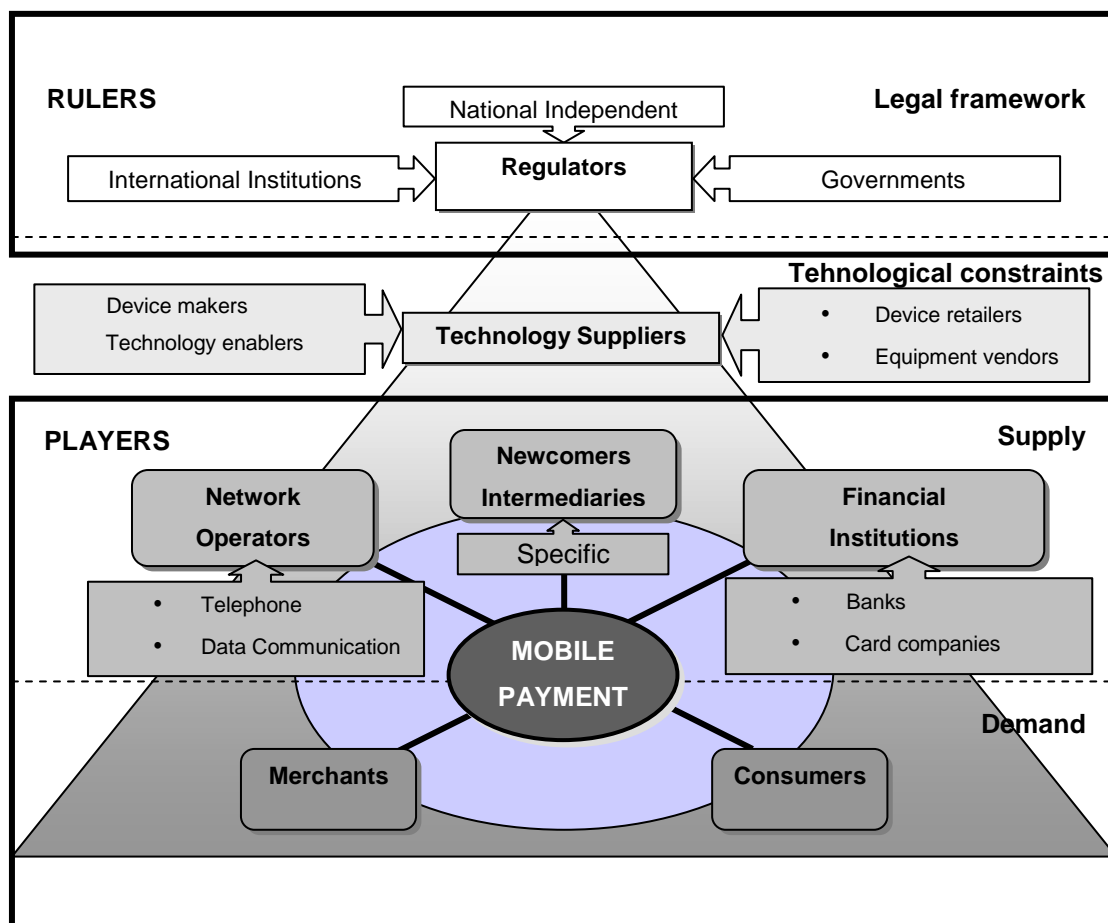


Figure 22: The Mobile Payment Arena

This figure shows that there are two groups of actors: the rulers and the players. Then, each group is classified according to the types to which they belong: legal framework, technological constraints, supply and demand. The triangle can illustrate the number of actor in each group. In fact, they are many more consumers and merchants than regulators. The circle represents the potential «active» links between the players during a mobile payment transaction.

As we can see, the five main players in the mobile payment arena are consumers, merchants, mobile operators, newcomers/intermediaries and financial institutions. On one hand, the presence of a demand, represented by consumers and merchants, is essential. However, on the other hand, depending on the system in use, the supply can take on many different forms as network operators, newcomers/intermediaries and financial institutions compete, interoperate, co-operate. Therefore, their presence

depends upon if the mobile payment solution asks for an intervention of one, two or all supply actors.

3.4.4.1 A Description Of Actors

The objective of this overview is to introduce the different actors involved in the mobile payment arena. Merchants and consumers generate the demand of mobile payments.

- **Merchants** want the payment process to be transparent to the user, as this encourages greater usage and/or propensity to complete a purchase. They also want any payment scheme to facilitate swift and easy completion to ensure they get paid on time [58]. They hope that a mobile payment system can also improve consumers' loyalty.
- **Consumers** represent the major target of all mobile payment initiatives. They decide if they want to use a mobile device for monetary value transactions. Their main expectation is that their payments have to be fast, easy, personalized, and secure. Most of them already possess a mobile handset. The phenomenal success of the Short Messaging Service (SMS) and USSD highlights the appetite for non-voice services on mobile device. Therefore, mobile payments will play a very important role if the consumer asks for new value added mobile applications. The supply of mobile payments is composed mostly of service providers coming from different industries. Network operators, financial institutions and newcomers/intermediaries will try to provide their solution to the mobile payment issue.
- **Network operators** manage the mobile communication infrastructure; enable mobile telephony and data communications. Moreover, some of them already provide a wired network for electronic payment transactions between business premises and banks' financial systems. A technology distinction has to be made to provide an overview of the different family of actors involved. The convergence of voice and data brought two types of competing or complementary technologies:

- Telephony technologies (GSM, GPRS, UMTS, ...)
- Data communication technologies (WLAN, Bluetooth, infrared, RFID, ...).

Network operators are natural candidates for providing payment services since they are already involved in billing for voice and data transport services [59].

Moreover, they have the desire to recoup the cost of the UMTS license which makes them very interested in taking over the mobile payment market with the idea of generating revenue with payment transactions.

- **Financial institutions** are primarily concerned with ensuring the integrity of the payment system and reducing the risk of fraud. They can be a bank, a card company, a clearing house or all at the same time.
- **Newcomers/intermediaries** principally exist because of the missing standard that should have been chosen by network operators and financial institutions. Actually, the technology to enable mobile payment and the demand for such service are there, but the supply is late to emerge. Therefore, newcomers/intermediaries' objective is to propose a well-integrated solution in the current mobile payment market with the current popular technologies in use such as SMS (Short Message Service) and USSD (Unstructured Supplementary Service Data). They use the mobile communication network to transmit the data and control the veracity of the payment process with a bank or card company. Intermediaries usually act as a third-party between financial institutions and network operators. To illustrate the importance of these new actors, we can look at Paybox, which already has 10,000 merchants and 750,000 subscribers for its m-payment service across Europe [60].

Other actors are in the background, but they still have their importance. They are the most powerful entities and they can easily influence the market of mobile payments. Despite being totally passive for mobile payments, they can be considered facilitators of the various mobile payment models [61]. They do not affect the real-time transaction, but they draw the future of mobile payments.

- **Regulators** have the role of making the rules and controlling their application. The existence of network effects calls for interoperability between the systems of different network operators. This interoperability can only be achieved by cooperation. It contains, however, the possibility of collusive behavior to the disadvantage of customers. Therefore, a special regulator supervises many network industries. Traditionally, regulation of payment systems has been a part of banking regulation and/or monetary policy. For example, California has started to regulate the use of mobile phones as payment devices. That regulation, in addition to the expected federal regulation, applies to any non-telecommunications charges placed on a telecommunications bill, including wireless bill [62]. Other institutions, such as standardization groups, are also very important because they will make the market more accessible to their followers.
- **Technology suppliers** invent and provide new technologies to the mobile communication market. Their role is crucial because they continuously improve devices that will enable an easier and more secure mobile payment process. To assess the role of the different actors in a selected market, Camponovo and Pigneur recommend to briefly but clearly describe the business model of each actor [63]. They adopted an ontology or framework for e-business models developed by [64] and represented in Figure 28.

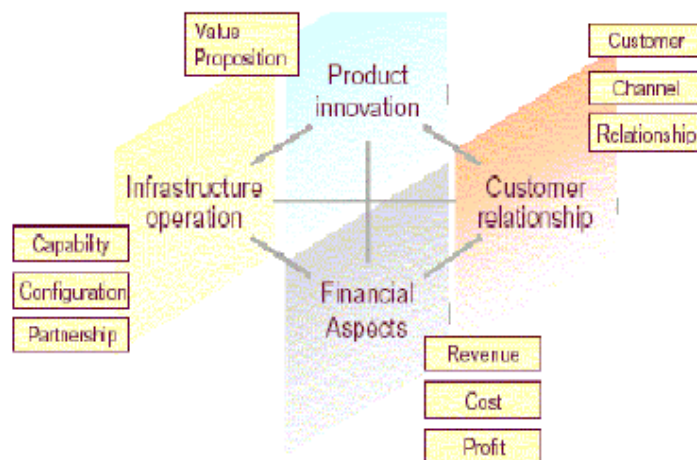


Figure 23 : Mobile Business Model Framework

3.4.4.2 Description Of Actors Using Business Models

































To succinctly illustrate the use of business models to describe actors, we propose to take the network operators as an example in Table 6.

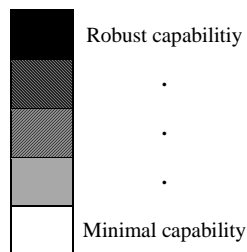
Table 6: Network Operators' Business Model

Value proposition	They operate mobile voice and data communication network. They mainly provide mobile telephony to end-users. Surrounding services like messaging (SMS), WAP and other network value-added services (content provider, location-based services, billing for third parties, ...) are also part of their offer.
Target customers	Telcos' targets are almost everyone from children to grandparents, including professionals such as business men.
Infrastructure	Telcos' main activities are network promotion and contract management, service provisioning and infrastructure operation. Telco's have a typical value network configuration. They partner with technology suppliers, other network operators (roaming), content providers and application providers.
Revenue model	They earn revenues from different sources such as fees for registration, monthly subscription, air time, volume of data transferred, the income from other activities like roaming and transaction for other parties.
Examples	Swisscom, Vodafone, AT&T, Tele2, Globalstar, ...

3.4.4.3 Actors And Roles

Table 7: M-Commerce Actors and Roles

Criteria	Banks	Credit Card Firms	Mobile Operators	Payment start-ups
<i>Motivation</i>	<i>Fear of staying behind</i>	<i>Add a new channel</i>	<i>New revenue and services</i>	<i>Business opportunities</i>
Mobile services skills				
Financial services skills				
Micro billing capabilities				
Macro billing capabilities				
Large end-user base				
Large merchant base				
Move quickly				
Able to expand quickly				
Sample company	SEB	VISA	Orange	Paybox



To describe some strengths and weaknesses of different actors to act as payment service provider, Buhan, Cheong and Tan use Table 7.

3.4.4.4 Four Appropriate Mobile Payment Models

Gartner Research proposes four model involving the different actors of the mobile payment arena [63]. These models are based on the needs and roles of these stakeholders.

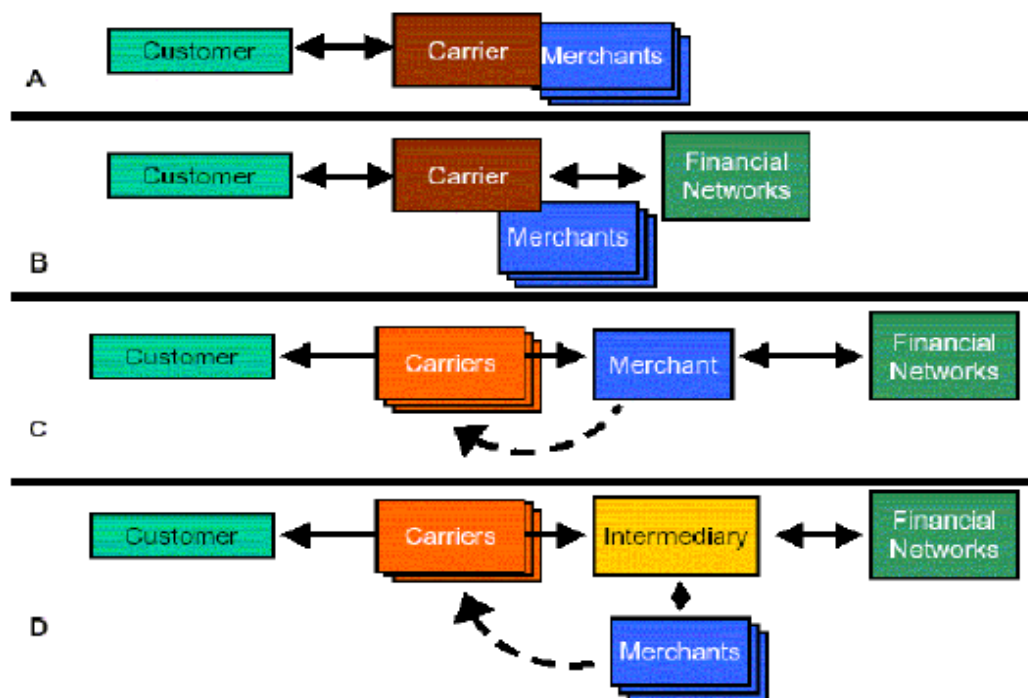


Figure 24 : Gartner's General M-Payment Models

Table 8 describes the different models introduced by Gartner.

Table 8 : Different Payment Models

	Given Names	Description	Comments
<i>A</i>	<i>Walled garden</i>	Customers buy directly from the carrier and the carrier servers as the sole provider of the content or operates as the "storefront" for other merchants.	Closed system. Invoices directly to the monthly wireless bill. Low value transactions to limit the financial risk for the carrier. Mostly adapted for digital goods.
<i>B</i>	<i>High-value garden</i>	Carriers choose to accept payments through the traditional financial network to avoid the financial risk coming from values greater than \$10.	Naturel extension of the walled garden model. Payments with a debit or credit card. Needs for carriers to establish relationships with banks and external payments processors.
<i>C</i>	<i>Buy direct</i>	Resembles the way PC-based online shopping and payments are transacted. Customers contact directly and separately with each merchant, who in turn must deal with the various payment processors.	Merchants can sell through multiple wireless carriers. Carriers are excluded from any revenue-sharing of the payment. A payment option can be the reverse-billed SMS. Then the carrier would charge the payment on the customers wireless bill.
<i>D</i>	<i>Mediated</i>	The intermediatery serves as the broker, formed the needed alliances and connections. The intermediary becomes the "glue" that facilitates commerce between all interested parties.	However, this role is not necessary played by an independent entity. A merchant, bank or even the carrier can perform the intermediation. This model minimized the interoperability limitations and the number of required relationships.

3.4.4.5 The Bank-Dominated Model

In this model, banks control the whole value chain, since telcos will only perform the data transport. Actually, mobile device would become another way for consumers to access their bank accounts.

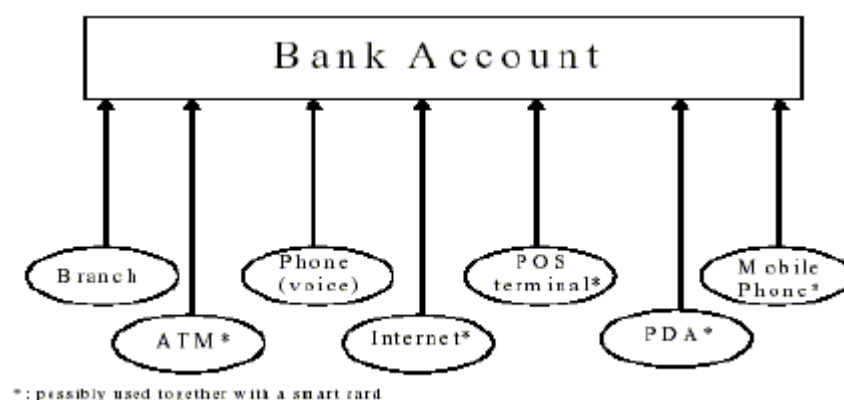


Figure 25 : The Bank-Dominated Model

The device marked with an asterisk may require the use of a smart card in order to make payments. This card would be issued by a bank to enhance security of data storage and transmission and allow strong identification [64]. Concerning the mobile device, there are two obvious solutions designed, such as the dual-slot phone or a separate payment chip embedded in the mobile phone.

In this case, banks have complete control over the customer relationship and the payment process. They will thus keep their supremacy in providing payment services. At the end of this paper there is a project sampled to give an example for the bank dominated model.

3.4.4.6 The Role Of Network Operators

The potential of mobile payment has already been demonstrated, but the role that network operators have to play is not very clear. They are already offering payment services, but if they want to become a real payment service provider, they will have to manage the financial risk and apply for a bank licence [65]. For this reason, it is legitimate to wonder what network operators will do. Krueger describes three different roles that telcos could play in the mobile payment market. Table 9 summarizes his scenarios.

Table 9: Different Roles for Telco

Communication Providers	Telcos simply stick to their current business which is not very profitable. Selling value added services like payment is more tempting to generate some extra revenues. Telcos will probably not stay out of the market.
Third-party billing systems	Telcos implement third-party billing on behalf of merchants. Such systems allow customers to rely on a trusted billing relationship with telcos. They generate more traffic but also get commissions on payments. The problem that comes with providing this service is the risk of the credit. In fact, Telcos have to manage the risk if the customers cannot pay for the goods purchased before the end of the billing period. Telcos have to take care of such issues as credit limits to prevent fraud. They have to create mobile payment roaming agreements with other national and international network operators. To reduce the risk, they have to increase the frequency of settlements like banks and established payment providers that clear and settle everyday.
Pre-paid solutions	Telco simply debits payments to a prepaid card/account. This slightly reduces the risk. However, difficulties appear with payment roaming. Telcos have to monitor each other to take into account the type of payment service offered (prepaid or billing), and how credit and fraud risks are handled. To provide prepaid solutions, telcos have to become either an Electronic Money Institution (EMI) or a bank. The use of prepaid cards for payments of goods and services provided by third parties makes it necessary to get an EMI licence. Managing prepaid accounts is equal to managing deposits. Therefore, such payment solution would force telcos to become banks.

These roles show mobile network operators going alone in the market of mobile payment. Another possibility would be to team up with a bank, to take advantage of the synergy from the technological knowledge of network operators and the financial experience of banks.

3.4.4.7 The Newcomers/Intermediaries Opportunity

Because mobile network operators and banks are not able to launch a successful initiative, new opportunities appear for others. These parties will be primarily intermediaries working with mobile networks and banks. Some of them might

acquire an EMI licence or even a banking licence. Therefore, network operators would have the advantage of not being bothered with payment regulations if they would work with financial intermediaries. These intermediaries would take the financial risk that network operators do not want to support.

However, for example, Paybox is almost owned by Deutsche Bank. This means that banks are also interested to work with intermediaries that would use their banking system.

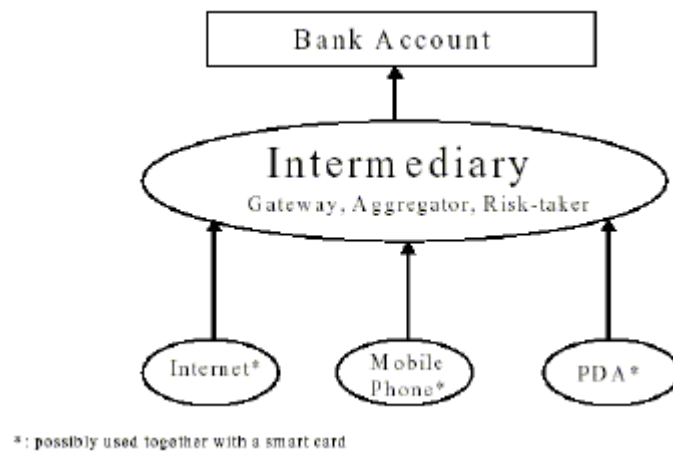


Figure 26 : The Newcomers/Intermediaries Model

3.4.5 .The Mobile Payment Issues

The objective of this section is to identify some mobile payment issues. Therefore, the idea will be to use what Tarasewich identified as a set of issues concerning the mobile e-commerce [66].

He classifies a number of possible issues within five categories¹ that we adapted for mobile payment:

- Mobile client issues
- Wireless communications infrastructure issues
- Other wireless technology issues
- Mobile payment application issues
- Mobile payment global issues

Using this categorization guides the identification of some issues that could concern the market of mobile payment.

3.4.5.1 Mobile Client Issues

The issues in this category concern the hardware and software of mobile clients.

The device's physical form

The question is to find out which device will be the most successful to support mobile payments. The device can be a mobile phone or another such as a PDA, a laptop or any wireless enabled device that could process securely a financial transaction over a wireless network.

The convenience of the device

Convenience and ease of use are very important in boosting the adoption of a new technology. People want something that they can easily use. If the device is too complicated, the majority of the potential users will be reluctant to subscribe to the system.

3.4.5.2 Wireless Communications Infrastructure Issues

The communication infrastructure enables mobile payment. There are many technologies today that can support wireless data transfers. In this section, some issues concerning the infrastructure are described.

The type of network

With all the new wireless communication technology available, the choice of using one network technology over another is difficult. Each technology brings its own advantages and disadvantages. Therefore, the infrastructure should support the most suitable technology, depending upon the type of payment. Today, *data communication networks* (WLAN, Bluetooth, ...) and *telephony networks* (GSM, GPRS, UMTS, ...) bring a new dimension to the issue. In fact, telcos are confronted with WLAN technology that could be a real threat for their existing business. Some of the mobile network operators are already anticipating the potential success of this technology by offering hotspots.

The network coverage

As discussed above, the need for coverage is different depending upon the type of mobile payment. For example, Bluetooth, RFID or infrared are adapted for *proximity payments* (e.g. vending machine) but not *remote financial transactions*. Then, mobile payment service providers have to choose the type of network which provides the most adapted coverage to support the payment transaction.

3.4.5.3 Other Wireless Technology Issues

The wireless technology brings its own new problem. The fact that data is transmitted in the air make it more vulnerable to eavesdropping.

Security in wireless environments

Wireless communications present the obvious problem that even unauthorized parties can access the flow of sensitive data transmitted. There are already some methods that reduce the risk that unwanted people or devices intercept communication. Natural protections could simply come from the complexity of the protocol (i.e. frequency hopping). However, encryption is essential to secure the data. In order to use wireless PKI systems for mobile payment, improvements in device processing power and network bandwidth will have to be made.

3.4.5.4 Mobile Payment Application Issues

Technology issues represent a first limit for the development of mobile payment. Then, application is another layer that can slow down the adoption of service. Applications should respond to the expectation of the consumers.

Micro payments vs. Macro payments

A mobile payment solution should be able to support either micro payments, macro payments or both. As discussed earlier, micro payments are a good target for network operators since credit cards are not adapted for small expenses. However, macro payments generate more revenues due to the bigger transaction fee that can apply to them. Therefore, macro payments are very attractive to most mobile payment service providers. The system should be adapted to the size of the payment; micro payments have to be fast and convenient, while macro payments have to be extremely secure.

Proximity vs. Remote

Financial transactions can be done either on a face-to-face basis or remotely. Network operators can benefit from a system that allows remote payments since they offer mobile service such as ring tones, games, horoscopes and other digital goods. Remote payments can also be used for e-commerce. Proximity payments enable classic financial transaction between two parties (B2C and P2P) present at the same place and same time. Mobile payment providers will have to choose the type of payment they want to support with their system.

3.4.5.5 Mobile Payment Global Issues

Universality and standardization

One way to promote mobile payments is to offer a universal way to pay. The possibility to pay anyone, anywhere, at any time should increase the chance of adoption of a new payment solution. Therefore, financial institutions and network operators are trying to form alliances to offer a standard.

Cost

The adoption of mobile payment systems depends directly upon who will have to pay the extra fee. Most consumers would not be willing to pay more without a real value added service. It will be very difficult for mobile payment service providers to convince consumers of the benefits if the cost of using their system is higher than classical solution.

Trust

For financial services, there is nothing more important than trust. People will not use a system if they do not trust it. Therefore, security and chargeback policies are factors that can improve the confidence of the users. After experiencing a bad situation during a financial transaction, the consumer will certainly drop mobile payments forever. Moreover, it appears that consumers prefer to see their financial data consolidated in banks[67]. This proves that customers care about who control their financial data.

Regulation

Network operators and newcomers are likely to be the actors most concerned about new regulation. In fact, banks are already strictly regulated. Mobile network operators tend to offer more financial services, so they have the choice of either extending their current billing services, or applying for an EMI licence and becoming a bank .

3.5 Conclusion

It is necessary to understand the difference between m-commerce and e-commerce. Those m-commerce service creators will succeed that offer services that adapt to the unique attributes of mobile devices as well as to the user's expectations. For the formation of long-term m-commerce strategies it is important to know what the state of the art solutions and emerging enabling technologies are.

Operators must have a good knowledge of regulatory, technological, security or market related issues. Operators have to know their own competence and choose the roles in the business model that suit them best. They have to examine the market for potential competition and decide which players are experienced and trustworthy enough to be their partners in building a profitable m-commerce solution. As we could see, the market for mobile payments is very immature, unpredictable and open for competition or collaboration between mobile payment service providers.

The most likely scenario to pass will be that mobile network operators and financial institutions will collaborate to offer a standardized solution. However, it seems customers are not yet ready to adopt en masse such a payment scheme.

In the meantime, mobile payments could possibly be offered for some niche services, such as vending machine or parking meters. For now, mobile payments solutions would be most accepted by consumers for e- and m-commerce.

Even if most of the current issues of mobile payment are solved, there is nothing that guarantees that consumers will adopt such a means of payment. Therefore, it is too early to predict what is going to happen on this market since even the mobile payment service providers are still looking for a standard solution that would be accepted by everyone.

4 CASE STUDY : MOBILE BANKING

4.1 Mobile Banking

Mobile banking can be defined as a portfolio of services that are offered by a financial institution on the Internet and which are available for the mobile user. These include at least balance checking but currently also the use of bank transfers and brokerage have started to increase in volume. For instance, for MeritaNordbanken an average user of the electronic banking uses services 4.1 times per month (Tainio, 1999). The total number of users is 1.2 million, majority of which have mobile terminals.

Another interesting remark is that 69 % of the exchange transactions that are made via MeritaNordbanken are made through electronic services. In addition, the prices for using the mobile banking are currently very low, (\$0.6/month + price of a data call). As exchange transactions sometimes require proper timing, it can be assumed that mobile transactions can be often used.

4.2 A Business Model For Mobile Banking

4.2.1 Introduction

In today's business environment, with so many deadlines to fulfill, appointments to meet and meetings to attend, you are hard pressed for time. Don't you wish you could do all your activities while traveling from one meeting to another?

Now you can access your bank account and conduct a host of banking transactions and inquiries through Mobile Banking service. You can check your balance, stop a cheque payment, or even pay your utility bills. Mobile Banking service gives you account information and real-time transaction capabilities from the mobile phones at a true "anywhere, anytime, anyhow" convenience. All this through SMS and USSD Service. This kind of Banking brings your bank accounts to your fingertips. It works

using Short Messaging Service (SMS) technology. With this services' total confidentiality and security you can perform a wide range of query-based transactions from your mobile phone, without even making a call.

Finally an account that travels with you. In this case study ,this service is to be introduced. All usage scenario and benefits , application development steps , data transaction performing steps and infrastructure is given in detail.

4.2.1.1 Services Offered and Usage Scenario

The whole mobile banking solution will be composed of different banking services. Every service will be developed as a separate prototype and at the end they will be integrated into a mobile banking system.

Services Offered

The services to be offered through Mobile Banking may be:

Balance Inquiry

Through this service, a customer can check his current bank account balance, anytime and from anywhere.

Money Transfer

Through this service, a customer can transfer money to his/her account either at the same bank or different bank.

Bill Payment

Through this service a customer can make payments of his/her bills.

Credit Card Payment

Through this service a customer can make payments of his/her credit cards.

Interest Rates

Through this, a customer will be able to view updated Interest Rates.

Exchange Rates

Through this, a customer will be able to view updated Interest Rates.

Transfer Funds

Through this, a customer can transfer funds across his/her account.

Last Five Transactions

Listing Through this service, a customer can know his last five transactions anytime and from anywhere.

Change Operative Accounts

Through this service, a customer can change his/her operative/default account. By this customer can do transactions from his/her another account.

Change PIN

Through this, a customer can change his/her PIN No.

How to Use

Mobile Banking operates through Short Messages. You will need a mobile phone enabled for SMS. If you already activated the Mobile Messaging service, you do not need to do this again. This is a one time activity & has to be done only while activating this service. Table 10 gives a list of different types of transactions to be done through mobile banking using SMS.

How to Send a Transaction

1. The telephone number may match with the account number.
2. *100# or *102# etc. makes the customer to access to the Mobile Bank transaction menus.
3. The required data can be entered using the mobile handset. The user can browse other menus without payment.
4. If required, then the user can be authenticated and authorized by forcing to enter username and password.
5. .The smart SIM cards can help for identification, signing transactions, storing sensitive data and related service parameters. Also they facilitates displaying the approved data on the handset.

How to Read Replies

In a few seconds after sending message you will hear a beep on your mobile phone, it means that the information you want has arrived. To read the information, go through the menu & select the "Read Messages" option. The message will then appear on your Mobile Phone screen.

Table 10: Different types of Transactions

Transaction Type	Brief Description	SMS/Keyword to be sent	Reply Received.
Menu	Will display the list of all the options available with the description.	*100# or *102# etc.	1.Balance Inquiry 2.Money Transfer 3.Bill Payment 4.Credit Card Payment 5.Interest Rates 6.Exchange Rates 7.Transfer Funds 8.Last Five Transactions 9.Change Operative Accounts 10.Change PIN
Balance Enquiry	Will give you the available balance in the default/operative accounts that are linked to your customer identification number.	1	Balance in A/c (your A/c No) is Rs. (Amount) Effective Available Balance is Rs (Amount)
Money Transfer	Will give you availability to transfer money to his/her account either at the same bank or at different bank.	PAY(Account No) (Pin No) (Amount)	(Amount) transferred successfully. Your reference no is (Ref No)
Bill Pay	Pay your Utility Bills.	PAY(Utility Code) (Pin No) (Amount)	Your (NickName) Bill of Rs. (Amount) Paid successfully. Your reference no is (Ref No)

Credit Card Payment	Pay your credit cards.	PAY(Credit Card Code) (Pin No) (Amount)	Your (NickName) Bill of Cr. (Amount) Paid successfully. Your reference no is (Ref No)
Interest Rates	Latest & updated Interest Rates.	5	Displays the Interest Rates.
Exchange Rates	Latest & Updated Exchange Rates	6	Displays the Exchange Rates
Transfer Funds	Transfer Funds from one account to any of your account.	TRN(A/c No)(PIN No)(Amount)	Rs. (Amount) transferred successfully to (A/c No.) Note down your reference no (Ref. No)
Last 5 Transactions	Will give you information on the last five debits/credits made to your account.	8	Balance in A/c (Your A/c No) is Rs. (Amount). Transactions: (Last 5 Transactions).
Change Default A/c	Change your default A/c to any other account.	CHAC(new Account)	Your default account no is now (A/c No)
Change PIN	Change your PIN Number.	CHPIN(OLD PIN)(NEW PIN)	Your new Pin No. has been successfully updated to (PIN NO).

4.2.1.2 Payment Method

Payment is an important issue when it comes to adoption and acceptance of services by the customers. With the payment service specified in this project the customer can turn his mobile phone into a payment device and use it to pay for items and services at a real or virtual point of services subsequently. For payment of a chosen item he gets a purchase order by the merchant & banks, signs it with his private key and sends it back. The payment is safe, easy and quick. As the payment is offline and the service provider is only involved in the clearing process the transaction costs can be

kept low. The user can even stay anonymous if he wants to. Thus the micro or the macro payment from debit or credit card using Mobile Banking Service is the perfect enabling service for many other m-commerce services that involve the transfer of money .

4.2.1.3 Mobile Operator and Value Chain

The operator should position himself in a key role in the value chain by participating in the revenues accrued by Mobile Banking Services over its network. Those revenues will be significantly higher than the sheer increase in airtime charges. In order to achieve this a mobile operator should exploit its strengths (brand name, customer base, infrastructure, price control, etc.) effectively. The Bank also has some influence about the development of the protocol for data communication between the operator Application server and Bank web server.

4.2.1.4 Alliances

The most feasible scenario rests on appropriate partner-ships and business alliances, which are based on revenue sharing, with a key role for the operator as shown in the following figure.

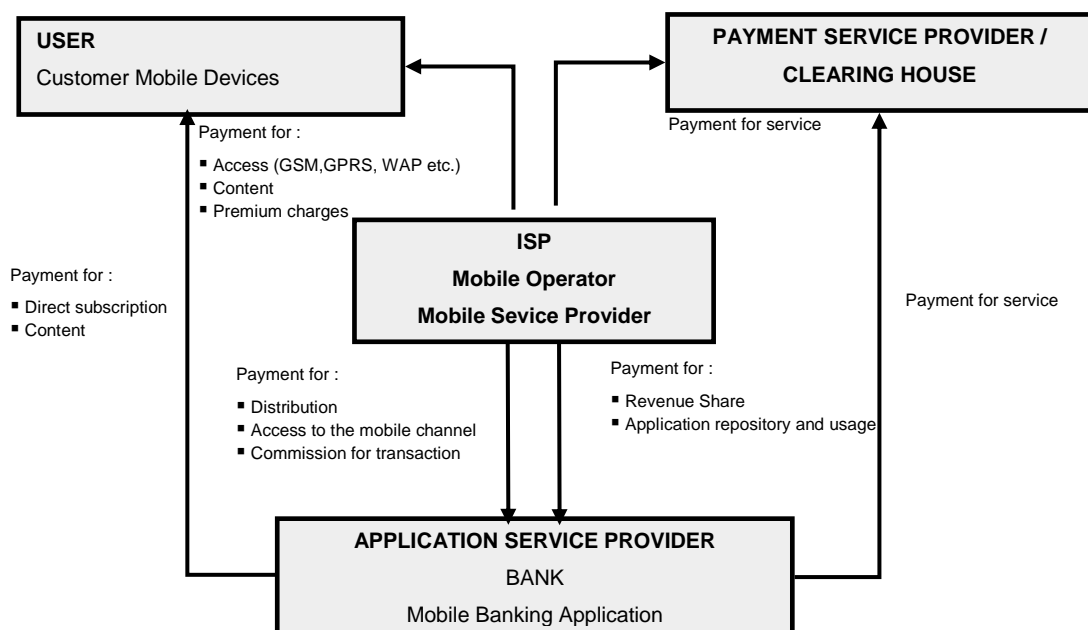


Figure 27 : Business model for Mobile Banking Service

4.2.1.5 Players

The main players that could participate in the mobile banking value chain are the user, who decides about the transaction type, the ISP providing access to the Bank, the Bank supporting the financial transactions and the mobile operator that provides the network as well as the portal.

4.3 A Prototype for Mobile Banking

Checking account balance on mobile phone :

Mobile banking is the fastest developing part of mobile commerce due to its convenience. In our case study for mobile commerce, a prototype of mobile banking has been developed in cooperation with one imaginary bank. The whole mobile banking solution will be composed of different banking services. Every service will be developed as a separate prototype and at the end they will be integrated into a mobile banking system.

One prototype will enable users to check their account balance. A user will have to send SMS to provide data collection on the USSD platform. With the receiving of data from telecom operator USSD application server, The Bank Application server generates a reference number regarding that transaction. Reference number and Password are encrypted on the SIM with specific security algorithms and sent to the Bank web server over TELCO Application server which can decrypt the data with the particular keys.

The bank Application server performs the transaction after the verification of the password and the reference number.

To develop and test the USSD services a prototype is designed. For testing purposes a SMS-C server, an USSD server and an Application server is supposed to be used for the gateway between mobile user and the bank. . Mobile service is developed as USSD application.

4.3.1 Project Description

This prototype enables users to check their account balance. When user wants to check account balance first he/she have to enter mobile banking service by entering

*100# into the phone. Then phone connects to the Internet through mobile network and reaches the bank menu. When connected to the server the phone displays bank names to choose and the user have to enter one of them. Then the necessary authorization and authentication queries required by the bank must be replied. He can than choose which account balance he want to check. And the data about his account is displayed on the phone. Displayed data may consist of account number, account balance, date of last change and what is the limit of this account. Finally, the user can log off, and close the connection to server. He can also make some transactions like EFT depending on the application developed.

Mobile Banking Service help customers to achieve banking transactions in an easy and secure way.

1. The telephone number may match with the account number.
2. *100# or *102# etc. makes the cumstomer to access to the Mobile Bank transaction menus.
3. The required data can be entered using the mobile handset. The user can browse other menus without payment.
4. If required, then the user can be authenticated and authorized by forcing to enter username and password.
5. The smart SIM cards can help for identification, signing transactions, storing sensitive data and related service parameters. Also they facilitates displaying the approved data on the handset.

Mobile bank service has five key features:

1. Development of a special applet that can be triggered by particular SMS.
2. Implement special security system on SIM. Thus the keys on SIM can encrypt the outgoing data and can be decrypted by the destination (Bank side only) only.
3. SMS message format between SIM to SMSC and SMSC to SIM
4. Development of USSD application or Web application by Bank.

5. Development of the protocol for data communication between TELCO Application server and Bank web server.

4.3.2 Overview of the Project

Project/Service has 6 parts in technical aspects:

1. Data Collecting
2. Data Submit: To send the data to banking server.
3. Transaction Confirm Request
4. Transaction Confirmation
5. Transaction Performing
6. Sending Back Receipt

4.3.2.1 Data Collecting

USSD will be used to query and buffer the information and transfer it to Web Server. When the user will press *100# this will come to USSD server. That will be transferred to Application server. Thus the application server will deliver menus to the mobile.

4.3.3 Menu Structure

The menu structure will be like this:

Main Menu 1. My Accounts

Main Menu 2. Money Transfer

Leaf Menu 1: EFT

Leaf Menu 2: Transfer to my account

Leaf Menu 3: Transfer to another account

Main Menu 3. My Investments.

Leaf Menu 1: Buying Funds

Leaf Menu 2: Selling Funds

Main Menu 4. Credit Cards

Leaf Menu 1: Pay Credit Card

Main Menu 5. My Payments

Leaf Menu 1: Pay Bill

Main Menu 6. First Login

4.3.4 Parameters and Messages

Parameters and the message format will be as follows:

EFT

*EFT [accountnumber] [accountnumber] [requiredtime] [cost]

Transfer to my account

*TMA [accountnumber] [accountnumber] [requiredtime] [cost]

Transfer to another account

*TOA [accountnumber] [accountnumber] [requiredtime] [cost]

Buying Fund

*IHA [accountnumber][fundcode][fundtype][fundcount] [requiredtime] [cost]

Selling Fund

*IHS [accountnumber] [fundcode] [fundtype] [fundcount] [requiredtime] [cost]

Pay Credit Card

*IKO [creditcardnumber] [creditcost] [accountnumber]

Pay Bill

*IFO [company] [date] [cost]

*ILK [ICCID]

First Login :

4.3.5 Inputs

Numeric Inputs:

[accountnumber] : 0 - 11 numeric characters

[creditcardnumber] : 0 – 16 numeric characters

[date] : 6 numeric characters

[fundcount] : 0 – 16 numeric characters

[cost]: 0 - 13 numeric characters

Alphanumeric Inputs:

[fundcode] : 0 - 6 alphanumeric characters (A,B...,Y,Z; 0,1...,8,9)

[creditcost] : 0 - 13 alphanumeric characters ([T], [D], [A] or numeric input 0,1,2,3,4,5,6,7,8,9)

Alphabetic Inputs:

[fundtype] : 1 alphabetic char. (E, Y, or space)

[requiredtime] : 1 alphabetic char. (S, G, or space)

[company] : 20 alphabetic characters

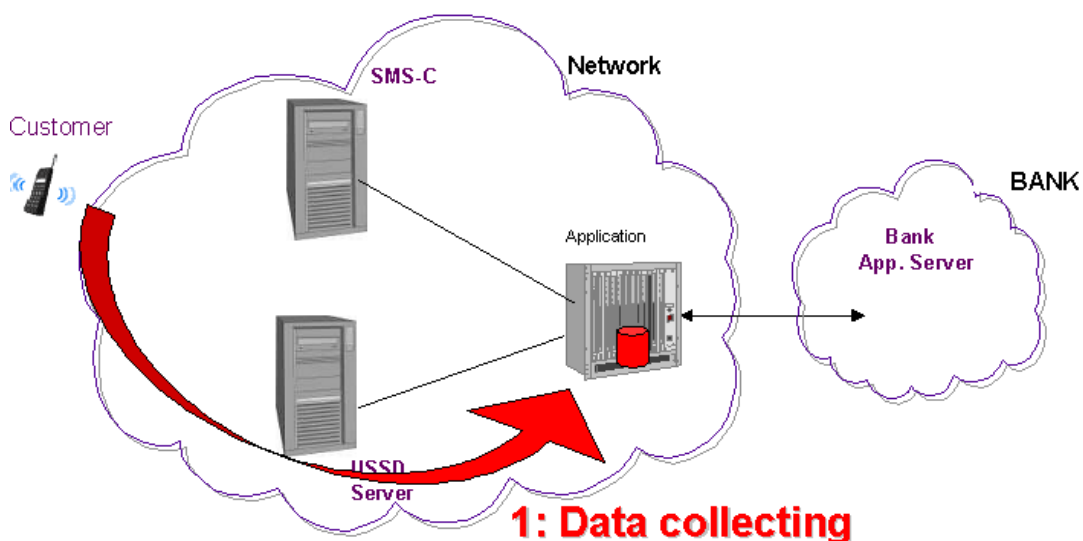


Figure 28: Data Collecting

Whenever it is pressed on the “6.First Login” menu on the USSD Application server, a special SMS will be sent to the SIM (user) that will contain FFFF...FFFF(12 bytes) at the place of reference number.

With the reception of this message with this reference number, an applet inside the SIM will be triggered that will read and get the ICCID number from the SIM.

Applet will add this ICCID (20 bytes) with the message type (MT = 02)(1 byte) and will form a 21 bytes data.

Applet will then send this 21 byte to “9203”, which is the service number. Application server will get this 21 byte and will forward to Bank side without any modification.

1.

Reference Number(FFF..FF) 12 bytes

 Sent by TELCO

2.

MT (1byte)	ICCID Number (20 bytes)
------------	-------------------------

 \Rightarrow 9203

4.3.5.1 Data submission

Data submission to the web server of the The bank. This is done over HTTPS. After data collection is done by USSD banking application, it will be forwarded to Bank. Bank will generate a Reference Number (RN) of 12 bytes and will forward to TELCO USSD Banking Application.

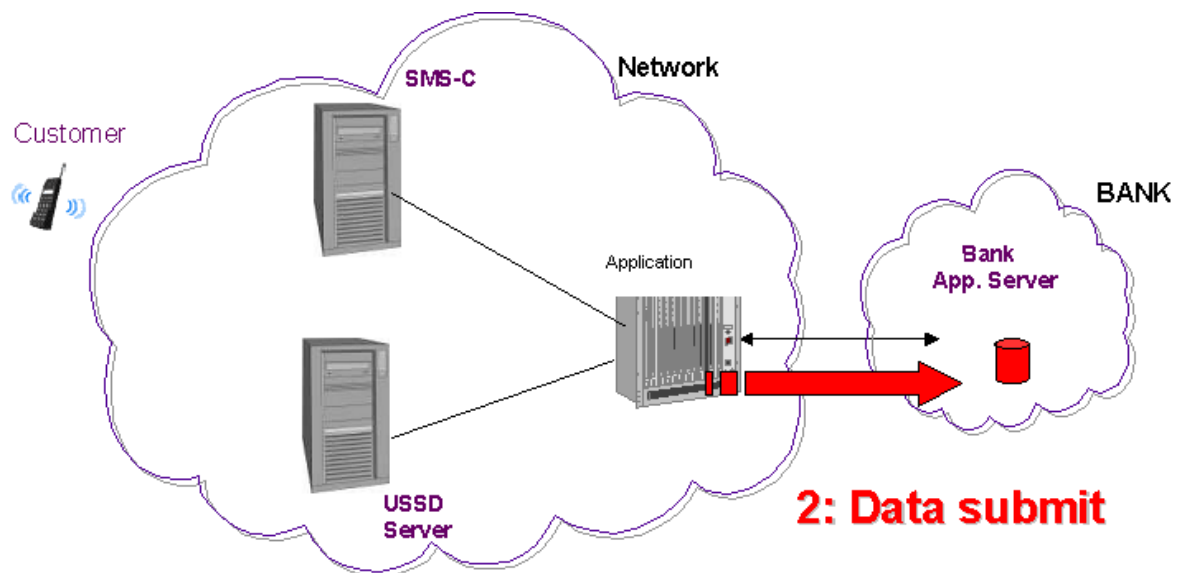


Figure 29: Data Submit

4.3.5.2 Transaction Confirm Request

With the receiving of data from TELCO USSD application server, The bank Application server generates a reference number regarding that transaction.

Banking Application will send this data with a special SMS so that it can trigger the applet inside the SIM.

With the arrival of this SMS, a pop-up menu will be on the screen of the Mobile Equipment (ME). There, the customer will be asked the following question:

(This question obviously be in Turkish.)

DO YOU WANT IT PERFORM THE TRANSACTION?

YES

NO

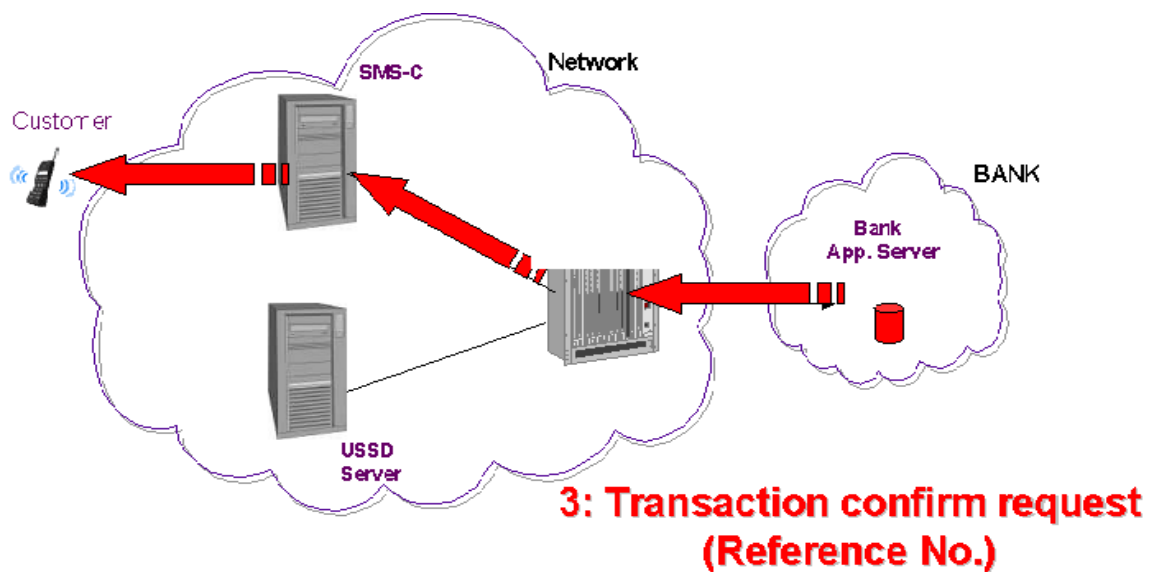


Figure 30: Transmit Confirm Request

4.3.5.3 Transaction Confirmation

Reference number and Password are encrypted on the SIM with specific security algorithms and sent to the Bank web server over TELCO Application server which can decrypt the data with the particular keys.

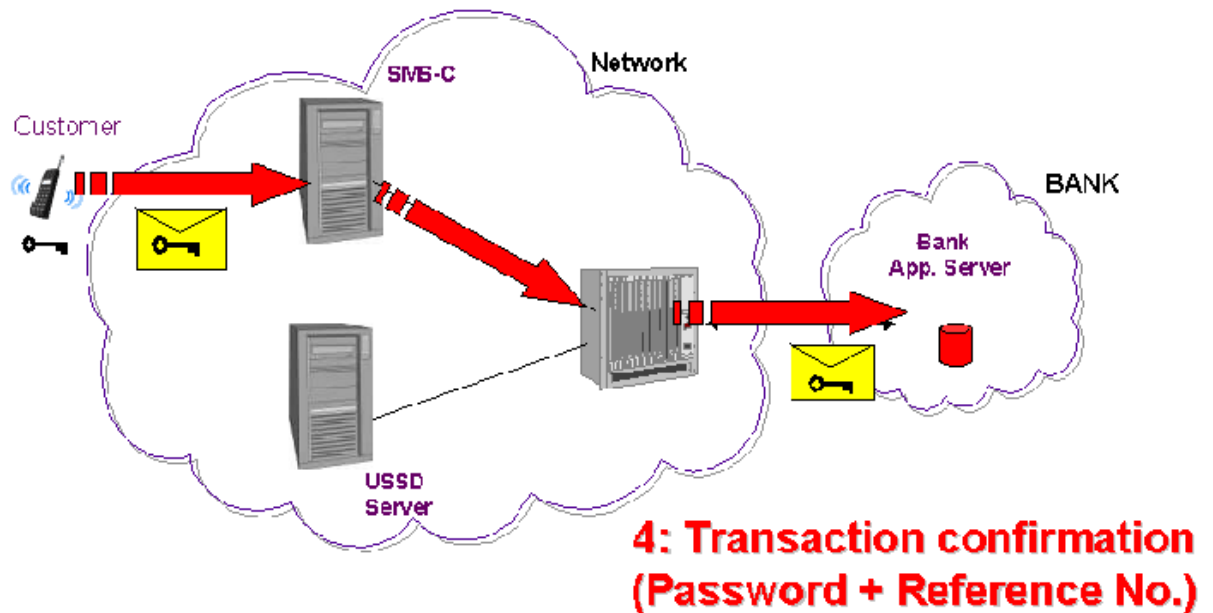


Figure 31: Transaction Confirmation

In Case Of "YES"

If it is pressed on YES, the customer will be asked the PIN number. This will be a 4 digit PIN and will be hidden. In case of pressing on "*" or "#" while typing the PIN, "MUST BE NUMERICAL INPUT 0-9" error message will be shown on the screen.

SIM will get this PIN and will add with the RN that came with the message and will form a 16 bytes data. This will be encrypted. Encryption method will be 3DES with 2 key and keys will be stored on the SIM file system. (Keys will be formed with a special algorithms defined by Bank and TELCO).

Message Indicator byte will be added with this encrypted data and will be sent to 9203 service number. And thus will be sent to the bank without any modification.

1.

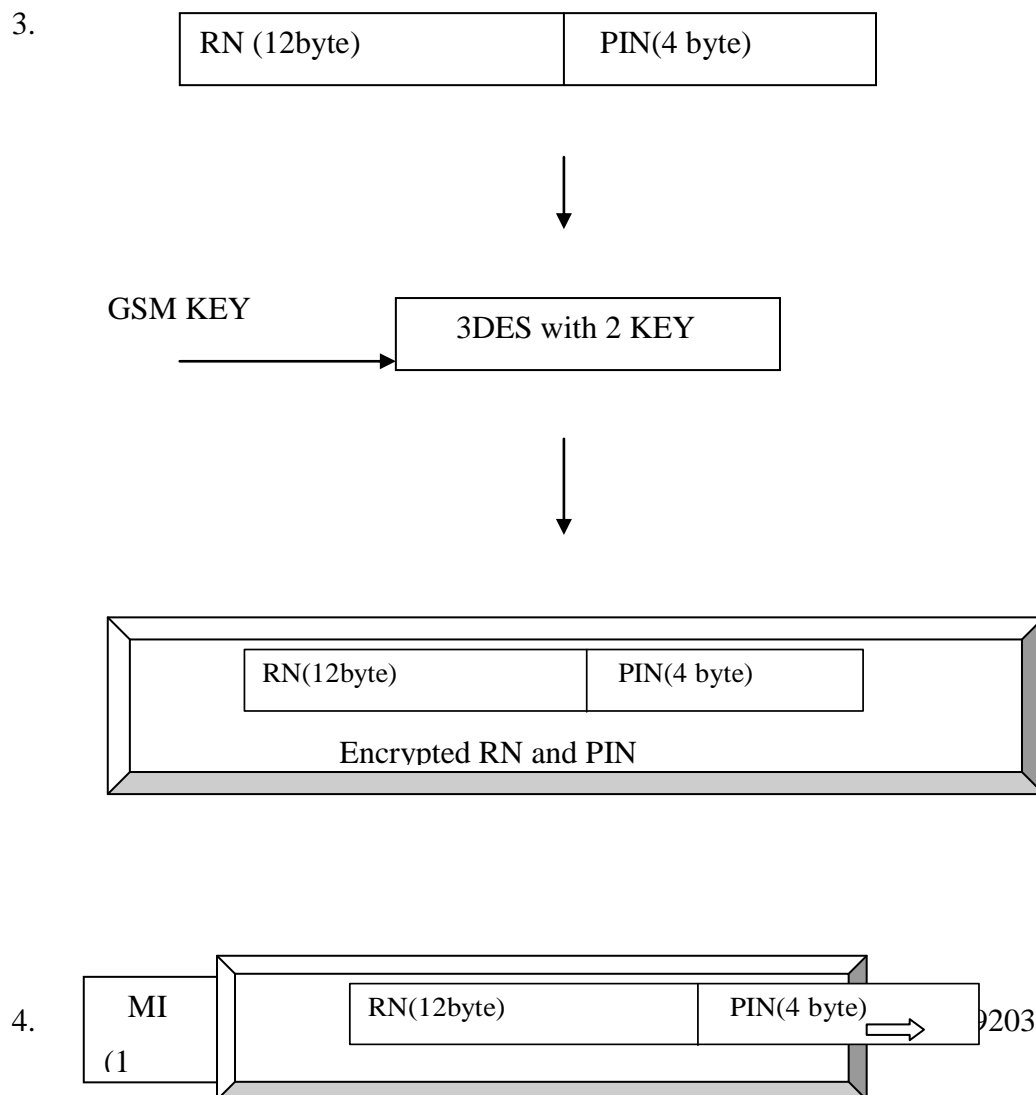
RN (12 byte)

.... Generated at the Bank side.

2.

RN (12 byte)

.... Send to SIM.



In Case Of “NO”

If it is pressed on No, only the RN and message indicator that came with the incoming SMS will be sent to 9203, and thus will be forwarded to the bank.

1.

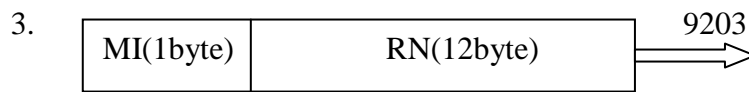
RN (12 byte)

 Generated at the Bank side.

2.

RN (12 byte)

 Generated at TELCO.



4.3.5.4 Transaction Performing

USSD application server will be the mid point of this project. Key features to use this USSD server is as follows:

- No need to put the application in the SIM
- No need to prepare “special SIM” (horizontal market)
- Flexibility in updating the application when needed

The bank Application server performs the transaction after the verification of the password and the reference number.

USSD application will get this message from the SMSC and will pass to web server. Web server will understand that this is a accepted message by the Message Type indicator (0x00). Web server will take all necessary action according to this accepted message. It will send a confirmation message to USSD. USSD application will deliver this message from 9230.

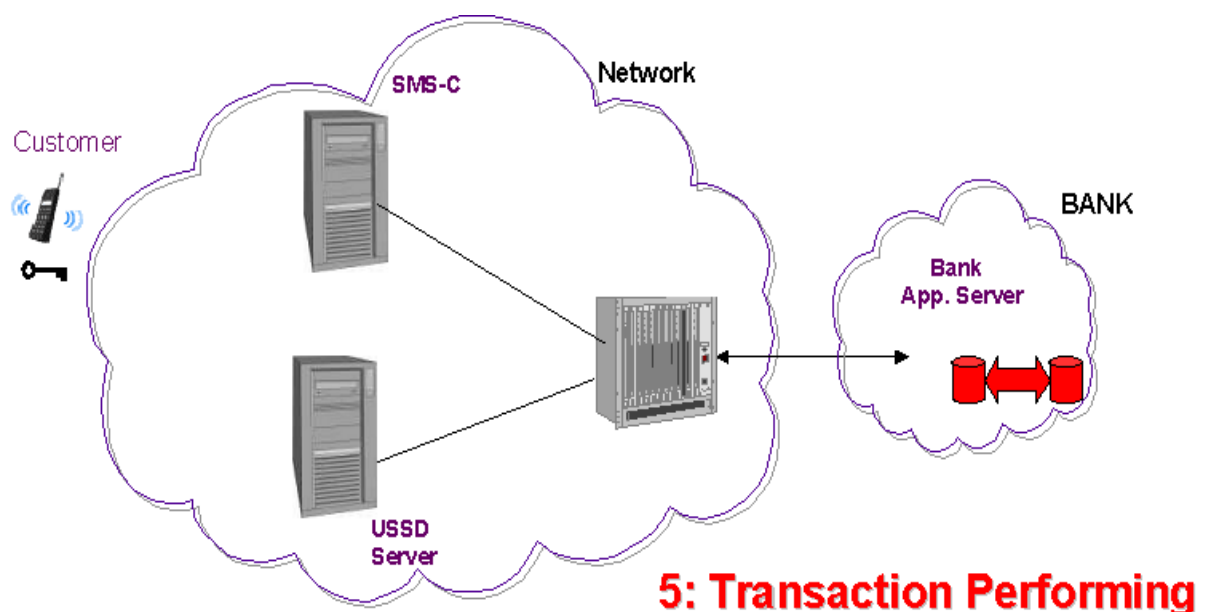


Figure 32: Transaction Performing

Data communication procedure between USSD Server and The Bank Web Server

USSD server will transfer data to the Bank application server in XML format.

Below is the data communication format between each server.

<APPN>

The Telco input App_Name is not modified while transferring. (6 byte)

</APPN>

<SEQNO>

The Telco input Sequence_Number is not modified while transferring. (6 byte)

</SEQNO>

<MSISDN>

The Telco MSISDN input is not modified while transferring. (12 byte)

</MSISDN>

<MENU>

Menu option may be 0 or 1.

If 0 then ,MSG consists of the SMS to send customer.

If 1 then ,MSG consists of a menu .

</MENU>

<MSG>

If MENU is 0 then ,MSG consists of the SMS to send customer.

If MENU is 1 then ,MSG consists of a menu .(If the customer has more than one credit card ,then there may be more menus listed.)

<MENU>

Menu options

</MENU>

<MENU>

</MENU>

.

.

.

</MSG>

4.3.5.5 Sending Back Receipt

After the transaction Bank sends back a report of the transaction.

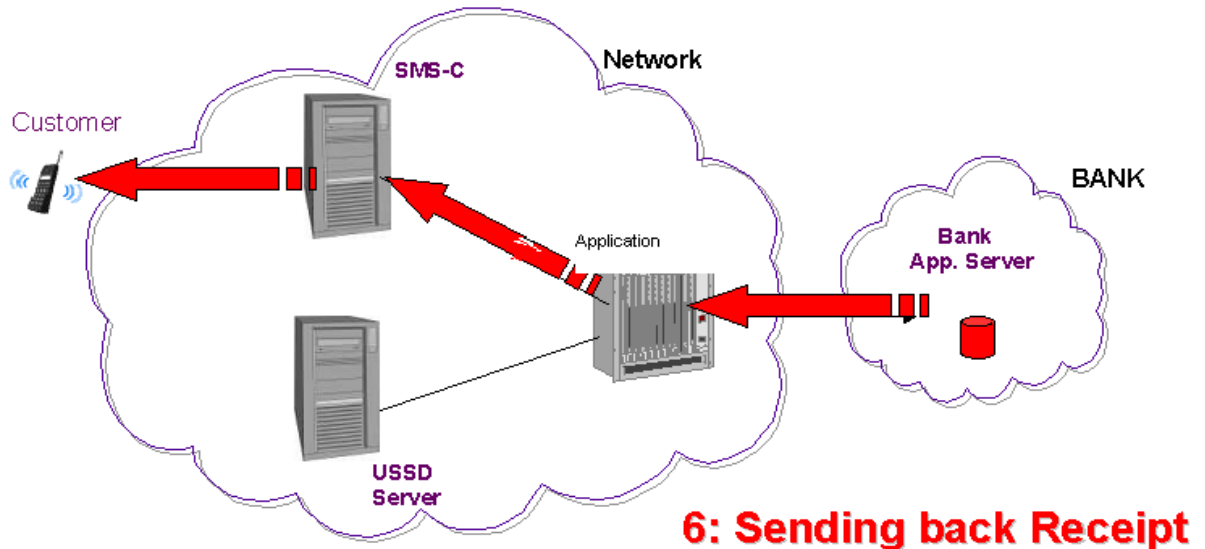


Figure 33: Sending Back Receipt

4.3.6 Conclusion

Over 12% of our Internet banking customers also use our mobile banking services. The response has been very good, primarily due to the availability of these services independent of any mobile operator. As of today mobile banking usage patterns still reflect over 95% of enquiry-based transactions. About 1% transactions are related to statement and chequebook requests and the rest relate to bill payments and demat services.

The biggest inhibitors in adoption of mobile banking services is the absence of on-line transaction based services with the offering that most of the banks have in their m-banking suite of products. Since more and more people are finding transactions through the Internet safer and faster, they would surely move to the SMS channel as the convenience is enhanced further on this channel.

Another reason is operator dependent offerings, where the registration process is cumbersome and the reach is limited to only the common customers of the two parties.

5 CONCLUSION

At this study, we defined a payment as a transaction of a monetary value from one party to another party. This can be done through one or many intermediaries, such as a bank or a card company. By enabling new technologies, especially mobile technologies, we saw more possibilities to initiate a payment transaction. The objective was to improve payment systems to approach a more frictionless process.

Traditionally, in the real world, the most popular modes of payments are cash, cheques, debit cards and credit cards. With the possibilities created by the Internet, a new generation of payments appeared, such as electronic payments, digital payments and virtual payments. Now, with the growing penetration of the mobile phone and the development of m-commerce, the mobile payment will become an uncontested mode for paying goods.

A logical evolution occurred in the monetary value transaction environment due to the progress of technology. In fact, at the beginning, payments were mostly conducted on a face-to-face basis (cash-, paper-, card-based). As technology progressed, remote transactions gained in popularity with the development of data wired networks (credit cards, e-payments). The current trend is now to implement mobile systems that can handle remote as well as face-to-face mechanisms with a single device.

The intention of this study is to detail all the technologies involved in mobile payments. Therefore we tried to contribute a mobile payment framework inspired from a mobile business application framework designed at chapter 4. We proposed all dimensions to classify different actors in this mobile payment ecosystem. First we defined mobile telecommunication technologies used in a mobile network infrastructure. Then mobile device and mobile security issues were explained in detail. Next we examined mobile operators', mobile application developers', content providers', regulators' views to create a business model. Finally we developed a mobile payment model according to this model.

As a result, we saw that it is necessary to understand both the mobile telecommunication technologies and the insight, which was gained from business model. Operators, financial institutions, and other m-commerce service creators must have a good knowledge of regulatory, technological, security or market related issues. They have to know their own competence and choose the roles in the business model that suit them best. They have to examine the market for potential competition and decide which players are experienced and trustworthy enough to be their partners in building a profitable m-commerce solution. As we could see, the market for mobile payments is very immature, unpredictable and open for competition or collaboration between mobile payment service providers. The most likely scenario to pass will be that mobile network operators and financial institutions will collaborate to offer a standardized solution.

REFERENCES

- [1] **Mobile Payment Forum**, 2002. Enabling Secure, Interoperable, and User-friendly Mobile Payments, *Mobile Payment Forum White Paper*.
- [2] **Cap Gemini Ernst&Young**, 2003. Mobile Payments: Money in Your Hands, *Telecom Media Networks*.
- [3] **Krueger, M.**, 2002, Mobile Payments: A Challenge for Banks and Regulators, *IPTS Report*, **Vol. 63**.
- [4] **Adrian, B.**, 2002. Overview of the Mobile Payments Market 2002 Through 2007, *Gartner Research* **R-18-1818**.
- [5] **Forrester Research Press Release**, «European Mobile Payments -- Can't Pay, Won't Pay, Says Forrester», May 2001.
- [6] **Jones, N.**, 2001. Paybox: Pan-European Mobile Payments, *Gartner Research*, **CS-14-2784**.
- [7] **Siau, K., and Shen, Z.**, 2003. Building Customer Trust in Mobile Commerce, *Communications of the ACM*, **Vol. 46, No. 4**.
- [8] **Buhan, D., Cheong, Y. C., and Tan, C.**, 2002. Mobile Payments in M-Commerce, *Telecom Media Networks*, *Cap Gemini Ernst&Young*.
- [9] **Muller-Veerse, F.**, 1999, Mobile Commerce Report, *Durlacher Research, Ltd.*
- [10] **EMC's e-searchwireless.com database**, Updated June 2001. Wireless Figures and Forecasts, «*Cellular Penetration By Region*»,
- [11] **Herzberg, A.**, 2003. Payments and Banking with Mobile Personal Devices, *Communications of the ACM*, **Vol. 46, No. 5**.
- [12] **European Mobile Forecast**, Retrieved August 9, 2004. Forrester's Annual Mobile Forecast Update
- [13] **Yeni Ekonomi Booklet**, Retrieved 30.January.2001. Sabah Gazetesi.
- [14] **USA Embassy**, 2001 *U.S. Third Generation Wireless Spectrum Activities and Memorandum For the Heads of Executive Departments and Agencies*
- [15] **BThaber**, 18-24.December.2000, page 3.
- [16] **Financial Forum**, 14.February.2001, page 16

- [17] **European Union Commision Report**, 2001. The Introduction of Third Generation Mobile Communications in the European Union: State of Play and the Way Forward, **Report No COM (2001) 141**, page 4.
- [18] **Ekonomik Danışmanlar Konseyi**, 2000, *Üçüncü Nesil Telsiz Teknolojisinin Ekonomik Etkisi Raporu*, page 3, 16.
- [19] **UMTS Forum**, 2001. A Regulatory Framework For UMTS, Report No.1, p.15-16.
- [20] **BThaber**, 18-24 December 2000, page 3
- [21] **BThaber**, 22-28 January 2001, page 8
- [22] **Devlet Planlama Teşkilatı**, 2000. VIII. Beş Yıllık Kalkınma Planı, paragraph 628-629, 1251-1252 and 1262, table 24.
- [23] Data on table are referenced from European Communications, August 2000, page 28.
- [24] **Cane, A.** 1999, BT Cellnet's GPRS trial at www.ft.com, retrieved 25th of June 1999.
- [25] **International Engineering Resources-Web ProForum**, www.iec.org/tutorials/umts/topic01.html, page 1
- [26] **SMS crosses over to mainstream**, Retrived 16 November 2000 <http://www.mobilesms.com/smsnews.asp>
- [27] **California Software Labs. TechCenter**, SMS (Short Message Service) - Technical Overview, *Systems Programming And Network Programming*.
- [28] **WAP Forum Consolidation**, <http://www.wapforum.org/>
- [29] **Mouly M., Pautet M.B.**, 1992. The GSM System for Mobile Communications.
- [30] **European Telecommunications Standards Institute**, 2001. www.etsi.org, checked 19.2.2001.
- [31] **www.3gpp.org**, Retrieved at 19.2.2001.
- [32] **GSM Technical Specification**, 1999. GSM 03.64 version (Phase 2+), Overall description of the GPRS radio interface, Stage 2, *ETSI*.
- [33] **GSM Technical Specification**, 1997. GSM 10.14 version 1.0.1, Digital cellular telecommunications system (Phase 2+), System Overview for 14.4 kbit/s Work Item, *ETSI*.
- [34] **GSM Technical Specification**, 1998. GSM 02.60 version 6.1.0, GPRS Service Description, Stage 1, *ETSI*.

- [32] **Ludwig, R. and Katz, R.H.**, 2000. The Eifel Algorithm: Making TCP Robust Against Spurious Retransmissions, *Computer Communication Review*, **Vol 30, No 1**.
- [33] **G. Montenegro, et al**, 2000. Long Thin Networks, *RFC 2757*.
- [34] **USSD Publication Zone**, www.mobileussd.com
- [35] **USSD Prepaid Roaming**, Retrieved at 2004. <http://www.telologic.com.sg/Tel-USSDPrepaidRoaming.html>
- [36] **Operator Servisleri**, Retrieved at 2004.
http://www.telsim.com.tr/servisler/operator_servisleri/GPRS/index.php
- [37] **3G, UMTS and WCDMA Technology** page from UMTS World.htm
- [38] **Rysavy, P.**, 1998. Planning and Implementing Wireless LANs. *Network Design Manual*, Retrieved November 1, 2001 from
<http://www.networkcomputing.com/netdesign/wlan3.html>
- [39] **Wireless LAN Security, 2001**. White Paper. Retrieved June 16, 2001 from the World Wide Web <http://www.wlana.com/learn/security.htm>
- [40] **Kesarev, K.** 1997. Security level and solutions in wireless and mobile data transfer. Seminar report. Retrieved November 20, 2001 from
http://www.tml.hut.fi/Opinnot/Tik-110.300/Tehtavat/mobile_wireless/security_2.html
- [41] **Harte, L., Levine, R., & Livingston, G.**, 1999. GSM Superphones, *McGraw-Hill*, USA.
- [42] **SIG Security**, 2001. Säkerhet vid trådlös datakommunikation (in Swedish). *Sweden Studentlitteratur*.
- [43] **Steele, R., Lee, C.-C., and Gold, P.**, 2001. GSM, cdmaOne and 3G Systems. *Wiley & Sons*, USA.
- [44] **Knight, W.**, 2000. 3G: Will 3G devices be secure? Retrieved from ZDNet UK, 23rd August.20.November.2001 from
<http://news.zdnet.co.uk/story/0,,s2080988,00.html>
- [45] **Costello, D.**, 2002. Preparing for the mCommerce Revolution - Mobile Payments, *Trintech White Paper*.
- [46] **Speedfacts Online Research GmbH**, 2001. mBanking – The Future of Personal Financial Transaction?
- [47] **Krueger, M.**, 2001. The Future of M-payments - Business Options and Policy Issues, *Electronic Payment Systems Observatory (ePSO)*, Background Paper **No.2**.

- [48] **Krueger, M.**, 2000. M-Payments and the role of telcos, *Electronic Payment Systems Observatory, (ePSO)*, Newsletter **No. 2**.
- [49] **Dahlberg, T.**, 2002. Consumers Talk Back: Interview Based Findings about Consumers' Willingness to Adopt Mobile Payment Solutions, *Helsinki School of Economics*.
- [50] **Watson R.**, 2000. U-Commerce: The Ultimate, Ubiquity, http://www.asm.org/ubiquity/views/r_watson_1.html
- [51] **Schapp, S., Cornelius, R.**, «U-Commerce - Leading the New World of Payments», A Visa International and Accenture White Paper, www.corporate.visa.com/av/ucomm/u_whitepaper.pdf.
- [51] **Camponovo, G., Pigneur, Y.**, 2003. Analyzing the m-Business Landscape, *Annals of Telecommunications, Hermes Science Publications*, **Vol. 58, No.1-2**.
- [52] **Seah, W., Pilakkat, S., Shankar, P., Tan, S. K., Roy, A. G., Ng, E.**, 2001. The Future Mobile Payments Infrastructure - A Common Platform for Secure M-Payments, *Institute for Communications Research, Systems @ Work Pte. Ltd*
- [53] **Adrian, B.**, 2002. Mobile Payments Consortia: What's the Difference?, *Gartner Research*, **SPA-15-5775**.
- [54] **Dahlström, E.**, 2000. The common future of wallets and ATMs? Mobile phones!, *Electronic Payment Systems Observatory, (ePSO)* Newsletter **No.1**.
- [55] **Carat, G.**, 2000. Mobile Payments: Alternative Platforms Players, *IPTS Report*, **Vol. 49**.
- [56] **Wrona, K., Schuba, M., and Zavagli, G.**, 2001. Mobile Payments - State of the Art and Open Problems, *WELCOM 2001*, Heidelberg, Germany.
- [57] **Salvi, A. B., Sahai, S.**, 2002. Dial M for Money, *WMC '02: 2nd ACM International Workshop on Mobile Commerce*.
- [58] **Krueger, M.**, 2002. Mobile Payments: A Challenge for Banks and Regulators, *IPTS Report*, **Vol. 63**.
- [59] **Cullen, D.**, 2003. Paybox Scraps M-Payment Service, <http://www.theregister.co.uk/content/59/29047.html>.
- [60] **Adrian, B.**, 2002. Overview of the Mobile Payments Market 2002 Through 2007, *Gartner Research* **R-18-1818**.
- [61] **Caldwell, K.**, 2001. Federal Government and States to Regulate Mobile Payments, *CommerceNet, The Public Policy Report*, **Vol. 3, No. 7**.
- [62] **Camponovo, G., Pigneur, Y.**, 2003. Analyzing the m-Business Landscape, *Annals of Telecommunications, Hermes Science Publications*, January - February.2003, vol. 58, no. 1-2.

[63] **Osterwalder, A., Pigneur, Y.**, 2002. An e-business Model Ontology for Modelling e-business, inProc. 15th Bled Electronic Commerce Conference (June 2002).

[64] **Krueger, M.**, 2001. The Future of M-payments - Business Options and Policy Issues, *Electronic Payment Systems Observatory (ePSO)*, Background Paper **No.2**.

[65] **Krueger, M.**, 2000. M-Payments and the Role of Telcos, *Electronic Payment Systems Observatory, (ePSO)*, Newsletter **No. 2**.

[66] **Tarasewich, P., Nickerson, R., Warkentin, M.**, 2002. Issues in Mobile E-Commerce, *Communication of the Association for Information Systems*, **No.8**.

[67] **Starita, L.**, 2000. ISPs, Wireless Carriers and Banks: Friends or Foes? Gartner Research, **COM-11-7054**.

APPENDIX A

The screen shots given only to sample mobile banking service transaction process. The first one is a prompt for user, and the second one is a reply from the service. The whole demonstration will be included as an attachment to this study.



APPENDIX B : MOBILE COMMERCE : MOBILE BANKING

I. Problem

The mobile telecommunication area is subject to an important debate which concerns the current and future successful technology in m-commerce.

This project is aim to enable the mobile technology and business strategy to develop a model for a mobile electronic commerce service: Mobile Banking.

The main problem is to define three dimensions to classify the different technologies in Mobile Banking. First, «Network» gathers the technologies used in a wireless network infrastructure. Then, «Device» represents the user wireless infrastructure. Finally, «mobile banking application» describes the technologies used mostly by mobile application developers, mobile application service providers and content providers.

II. Traditional Solution

Traditionally, in the real world, the most popular modes of payments are cash, cheques, debit cards and credit cards. With the possibilities created by the Internet, a new generation of payments appeared, such as electronic payments, digital payments and virtual payments. Now, with the growing penetration of the mobile phone and the development of m-commerce, the mobile payment will become an uncontested mode for paying goods.

A logical evolution occurred in the monetary value transaction environment due to the progress of technology. In fact, at the beginning, payments were mostly conduct on a face-to- face basis (cash-, paper-, card-based). As technology progressed, remote transactions gained in popularity with the development of data wired networks (credit cards, e-payments).

The current trend is now to implement wireless systems that can handle remote as well as face-to-face mechanisms with a single device.

III. Solution

In today's business environment, you can access your bank account and conduct a host of banking transactions and inquiries through Mobile Banking service. You can check your balance, stop a cheque payment, or even pay your utility bills. Mobile Banking service gives you account information and real-time transaction capabilities from the mobile phones at a true "anywhere, anytime, anyhow" convenience.

In our case study for mobile commerce, a prototype of mobile banking has been developed in cooperation with one imaginary bank. The whole mobile banking solution will be composed of different banking services. Every service will be developed as a separate prototype and at the end they will be integrated into a mobile banking system.

We have developed the two banking services in advance : *Checking My Account* (Bakiye Görüntüleme), *Transfer to My Account* (Hesaplarım Arası Havale).

Checking My Account (Bakiye Görüntüleme): This step will enable users to check their account balance. A user will have to send SMS to provide data collection on the USSD platform. With the receiving of data from telecom operator USSD application server, The Bank Application server generates a reference number regarding that transaction. The transaction ends with the display of all the accounts on the screen.

Transfer to My Account (Hesaplarım Arası Havale) : This step will enable users to transfer money from an account to the other account in different branch of the bank. A user will have to send SMS to provide data collection on the USSD platform. With the receiving of data from telecom operator USSD application server, a menu appears to ask for “*Transfer to My Account*” or “*Checking My Account*”. If “*Transfer to My Account*” is selected, then choosing from a number of account information and the amount of money is to be entered. The transaction ends with the display of all the transaction result on the screen.

1. Project Description

This prototype enables users to check their account balance and transfer money from one account to another.

When user wants to check account balance first he/she have to enter mobile banking service by entering *100# into the phone. Then phone connects to the Internet through mobile network and reaches the bank main menu. When connected to the server the phone displays branch names to choose and the user have to select one of them. Then the necessary authorization and authentication queries required by the bank must be replied.

In this study this authorization and authentication steps are skipped to simplify it. He can then choose which account balance he wants to check. And the data about his account is displayed on the phone. Displayed data may consist of account number, account balance, date of last change and what is the limit of this account. Finally, the user can log off, and close the connection to server.

He can also make some transactions like money transfer with this application. When the phone connects to the Internet through mobile network and reaches the bank main menu. When chosen “*Transfer to My Account*” option; he forced to chose two of his available accounts to make the transfer. The server the phone displays branch names to choose and amount of the money to transfer. All the rest is the same as “*Checking My Account*”.

Mobile Banking Service help customers to achieve banking transactions in an easy way secure way.

6. The id number is a unique number assigned per customer. In future work, telephone number may match with the account number.
7. The web browser makes the cumstomer to access to the Mobile Bank transaction menus. In future work, *100# or *102# etc. makes the cumstomer to access to the Mobile Bank transaction menus.
8. The required data can be entered using web browser as an XML application. In future work, the required data can be entered using the mobile handset. The user can browse other menus without payment.
9. The user is trusted site , he is not authenticated and authorized. In future work, if required, then the user can be authenticated and authorized by forcing to enter username and password.
5. Data send thorough XML, all tree site is simulated in one application. The user side, the telco operator side and the bank side communication is trough this

application. In future work, the smart SIM cards can help for identification, signing transactions, storing sensitive data and related service parameters. Also they facilitate displaying the approved data on the handset. The other security mechanism like encryption is also essential to secure the data. In order to use wireless PKI systems for mobile payment, improvements in device processing power and network bandwidth will have to be made.

Mobile bank service prototype has four key features:

1. Development of a special application that can be triggered by web browser.
2. Development of the structure for data communication between TELCO Application server and Bank web server.
3. Development of Web application according to the real Banking services.
4. Specifying customer information and account information format to be used for future work.

In future work, Mobile bank service will have five key features:

1. Development of a special applet that can be triggered by particular SMS.
2. Implement special security system on SIM. Thus the keys on SIM can encrypt the outgoing data and can be decrypted by the destination (Bank side only) only.
3. SMS message format between SIM to SMSC and SMSC to SIM
4. Development of USSD application or Web application by Bank.
5. Development of the protocol for data communication between TELCO Application server and Bank web server.

2. Overview of the Project

Project/Service has 6 parts in technical aspects:

1. Data Collecting
2. Data Submit: To send the data to banking server.
3. Transaction Confirm Request
4. Transaction Confirmation
5. Transaction Performing
6. Sending Back Receipt

3. Menu Structure

The menu structure will be like this:

Main Menu 1. Bakiye Görüntüleme

Main Menu 2. Havale Yapma

If you choose menu 1 item then you will encounter a sub menu which includes the account numbers you have within this customer id. You can proceed with selecting one of them to see your account info.

If you choose menu 2 item then you will encounter a sub menu which includes the account numbers you have within this customer id. You can proceed with selecting one of them to select the first account to make money transfer.

4. Parameters and Messages

Parameters and the message format will be as follows:

Bakiye Görüntüleme

Bakiye Görüntüleme ([id][account])

Havale Yapma

Havale Yapma ([id] [account1] [account2] [amount])

5. Main Program and Other Functions' Flow

Below is the list and purpose of all the subprograms used in this application. At the end there is a flow chart to show the relation and flow between subprograms. Appendix A includes all the codes in detail.

Function name: Welcome_jsp

Function Objective: Prompts to enter customer id.

Parameters: customer id as input.

Data Structure: "Customer id" string and "Demog" Customer table

Algorithm:

1. Prompts customer id text box
2. Enter customer id and submit
3. Find customer id in "demog" database
 - 3.1.If ok then go on TestOK
 - 3.2.If not then display "Müşteri bulunamadı"

Function name: TestOK.jsp

Function Objective: Displays the main menu. Prompts customer to choose one of the Menu items.

Parameters: Customer name and surname as output, menu as input

Data Structure: demog.getName(),demog.getSurname(),Inputs"Bakiye görüntüleme",
"Havale yapma"

Algorithm:

1. Display the Customer name and surname
2. Display the Main Menu
 - 2.1. If Bakiye görüntüleme Then gon on with AccountList
 - 2.2. If Havale yapma Then gon on with Havale1

Function name: Accountlist.jsp

Function Objective: Displays all the accounts on the screen.

Parameters: Customer name and surname as output, account list as input

Data Structure: demog.getName(),demog.getSurname(),acc.getBranch(),
acc.getAccount, acc.getCurrency()

Algorithm:

1. Display the Customer name and surname
2. Display the Account List
 - 2.1.Display the Branch
 - 2.2. Display the Account
 - 2.2.Display the Currency
3. Prompts to choose one of them
 - 3.1. If choose then go on with Amount.jsp

Function name: Amount_jsp

Function Objective: Displays the amount of the customer's account.

Parameters: Branch Name, Account, Currency, Amount as output

Data Structure: acc.getBranch(), acc.getAccount, acc.getCurrency(),acc.getAmount()

Algorithm:

1. Display the Account List
2. Prompts to return back to Main Menu

Function name: Havale1_jsp

Function Objective: Displays all the customer's accounts to make money transfer
"from " one of them.

Parameters: Branch Name, Account, Currency, Amount as input

Data Structure: acc.getBranch(), acc.getAccount, acc.getCurrency()

Algorithm:

1. Display the Account List
2. Prompts to choose one of them

Function name: Havale2_jsp

Function Objective: Displays all the customer's accounts to make money transfer
"to " one of them.

Parameters: Branch Name, Account, Currency, Amount as input

Data Structure: acc.getBranch(), acc.getAccount, acc.getCurrency()

Algorithm:

1. Display the Account List
2. Prompts to choose one of them

Function name: Havale3.jsp

Function Objective: Gets the amount to transfer between accounts. Prompts to user to
Approve the transaction.

Parameters: Branch Name, Account, Currency, Amount as output, Amount as input

Data Structure: acc.getBranch(), acc.getAccount, acc.getCurrency(), Amount

Algorithm:

1. Display the Account From
2. Display the Account To
3. Prompt to enter the amount
4. If ok then go on with Havale4

Function name: Havale4.jsp

Function Objective: Displays the result of the money transfer transaction.

Parameters: Branch Name, Account, Currency, Amount as output

Data Structure: acc.getBranch(), acc.getAccount, acc.getCurrency(), Amount

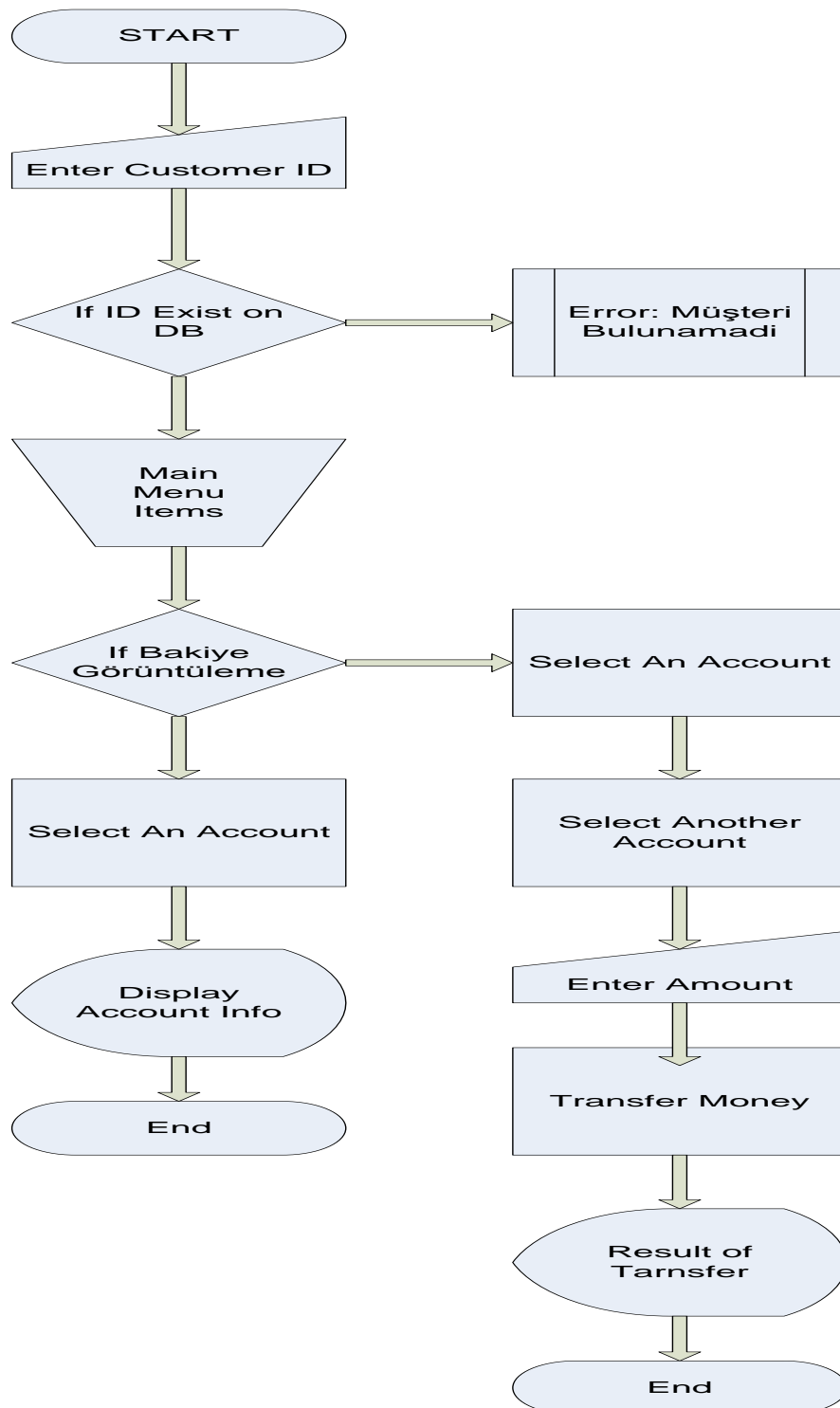
Algorithm:

3. Display the Transaction Result
4. Prompts to return back to Main Menu

Flow Chart:

The flow in the program is like :

User Request → Action → JSP



6. Inputs

6.1. Numeric Inputs

6.2. Alphanumeric Inputs

6.3. Tables

6.1. Numeric Inputs:

[Telephone] : numeric characters

[Id] : numeric characters

[Amount] : numeric characters

[Branch] : numeric characters

[Account] : numeric characters

6.2. Alphanumeric Inputs:

[Currency] : alphanumeric characters

[Name_text] : alphanumeric characters

[surname_text] : alphanumeric characters

[address_text] : alphanumeric characters

6.3. Tables

Demo Group Table

The screenshot shows the pgAdmin III interface. On the left, the 'public' schema is expanded, showing a tree of database objects. The 'demo' table is selected under the 'accounts' group. The right pane displays the table's properties and its SQL definition.

Özellik	Değer
Ad	demog
OID	17280
Sahibi	postgres
ACL (Erişim Kontrol Li...	{postgres=arwdRxt/postgres,=arwdRxt/postgres}
Birincil Anahtar	id
Satır (tahmin edilen)	1
Satır (sayılan)	3
Inherits tables	Hayır
Miras alınmış (inherite...	0
Has OIDs?	Hayır

```
-- Table: demog
-- DROP TABLE demog;

CREATE TABLE demog
(
    telephone numeric(10) DEFAULT 0,
    id numeric(9) NOT NULL DEFAULT 0,
    name_text varchar(50),
    surname_text varchar(50),
    address_text varchar(100),
    CONSTRAINT pk1 PRIMARY KEY (id)
)
WITHOUT OIDS;
ALTER TABLE demog OWNER TO postgres;
GRANT ALL ON TABLE demog TO postgres;
GRANT ALL ON TABLE demog TO public;
```


pgAdmin III Edit Data - PostgreSQL Database Server 8.0 (localhost:5432) - ...

	telephone numeric	id [PK] numeric	name_text varchar	surname_text varchar	address_text varchar
1	5334338456	100	sirin	mutlu	test
2	5321234567	200	ozge	caglar	test
3	5322227774	300	feridun	aktaş	test
*					

3 satır.

Accounts Table

pgAdmin III

Dosya Düzen Araçlar Göster Yardım

Sunucular (1)
PostgreSQL Database Server 8.0 (localhost:5432)
Veritabanları (1)
demo
Casts (0)
Diller (1)
Şemalar (1)
public
Aggregates (0)
Dönüşümler (0)
Domains (0)
Fonksiyonlar (19)
Tetikleyici Fonksiyonları (Trigger Func...)
Operatörler (0)
Operatör Sınıfları (0)
Sequences (0)
Tablolar (2)
accounts
Kolonlar (5)
branch
account
currency
id
amount
Kısıtlamalar (Constraints) (2)
İndeksler (0)
Rules (0)
Tetikleyiciler (triggers) (0)
demog
Kolonlar (5)
telephone
id
name text

Özellik Değer

Ad accounts
OID 17274
Sahibi postgres
ACL (Erişim Kontrol Li...
Birincil Anahtar branch, account
Satır (tahmin edilen) 3
Satır (sayılan) 9
Inherits tables Hayır
Miras alınmış (inherit... 0
Has OIDs? Hayır
Sistem Tablosu mu? Hayır
Yorum

Özellikler İstatistikler Bağımlı olduğu nesne Referans:

```
-- Table: accounts
-- DROP TABLE accounts;

CREATE TABLE accounts
(
    branch numeric(5) NOT NULL DEFAULT 0,
    account numeric(7) NOT NULL DEFAULT 0,
    currency varchar(3),
    id numeric(9) NOT NULL DEFAULT 0,
    amount numeric(15,2) DEFAULT 0,
    CONSTRAINT pk2 PRIMARY KEY (branch, account),
    CONSTRAINT fk FOREIGN KEY (id) REFERENCES demog (id) ON UPDATE REST
)
WITHOUT OIDS;
ALTER TABLE accounts OWNER TO postgres;
```

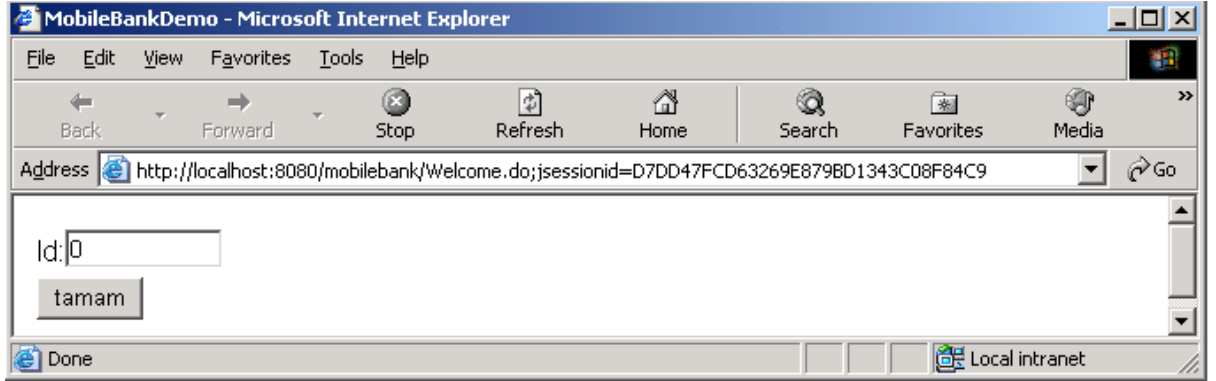
pgAdmin III Edit Data - PostgreSQL Database Server 8.0 (localhost:5432) - ...

	branch [PK] numeric	account [PK] numeric	currency varchar	id numeric	amount numeric
1	215	1122334	USD	100	100.00
2	215	1234344	YTL	100	198.00
3	215	2233445	YTL	100	902.00
4	235	335535	YTL	300	100.00
5	235	446677	YTL	300	550.00
6	235	1231231	USD	300	100.00
7	295	1234567	YTL	200	408.00
8	295	2345678	USD	200	100.00
9	295	3456789	YTL	200	692.00
*					

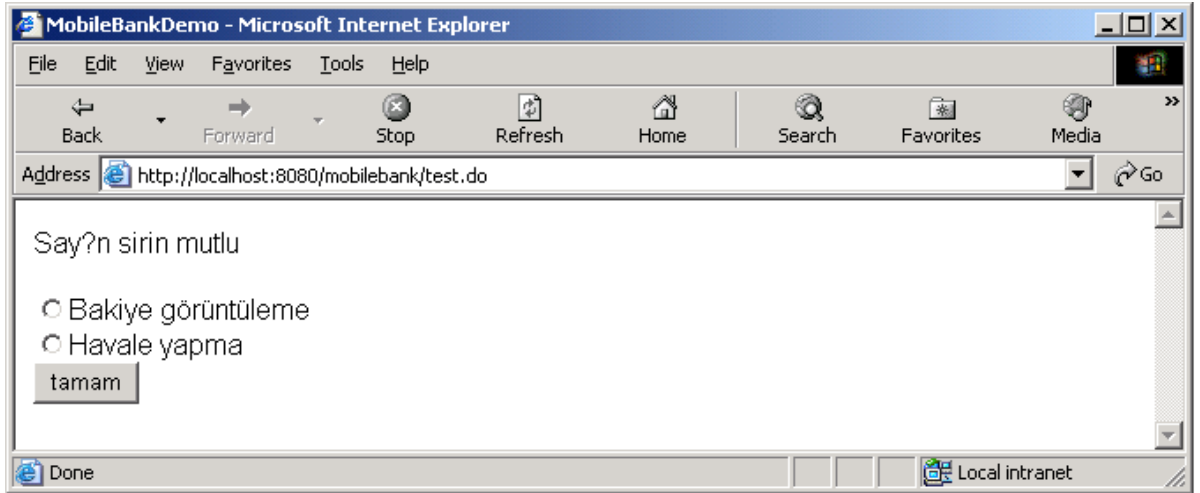
9 satır.

7. User Interfaces

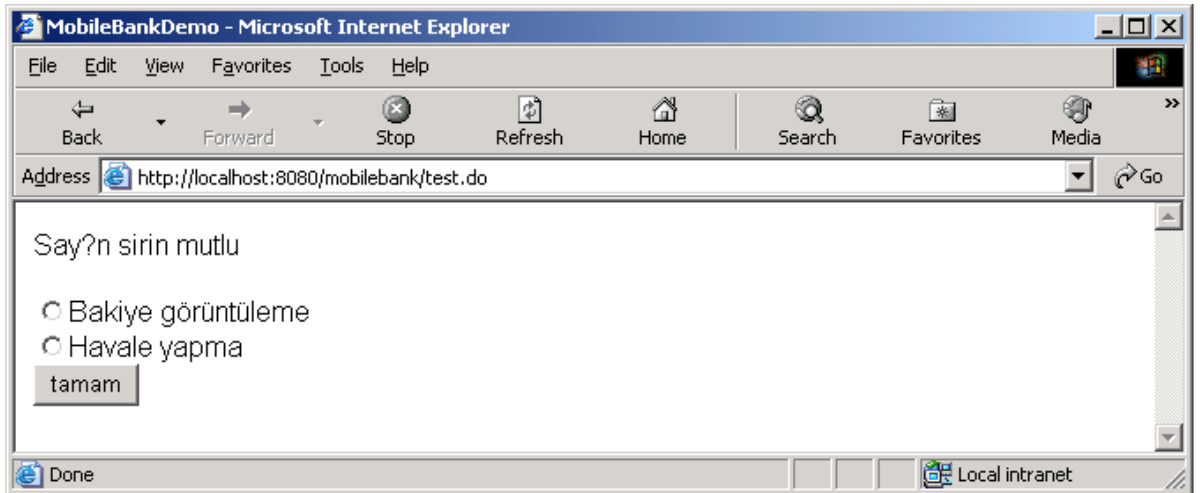
Welcome Screen :

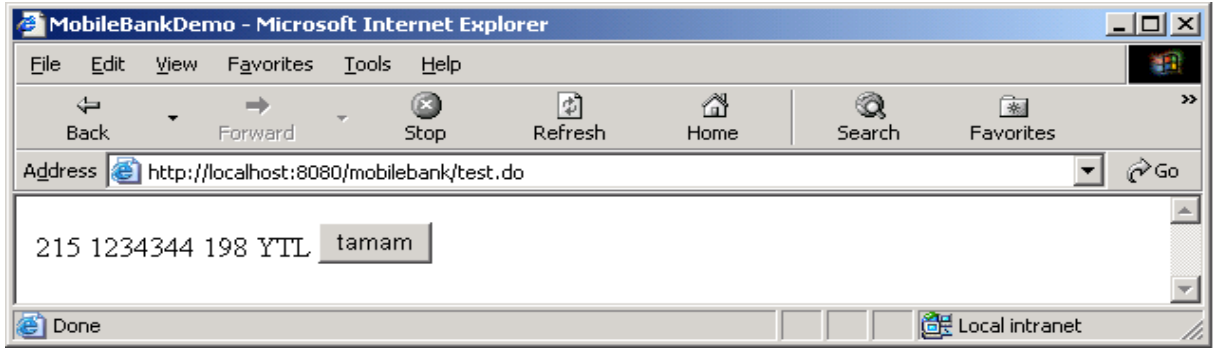
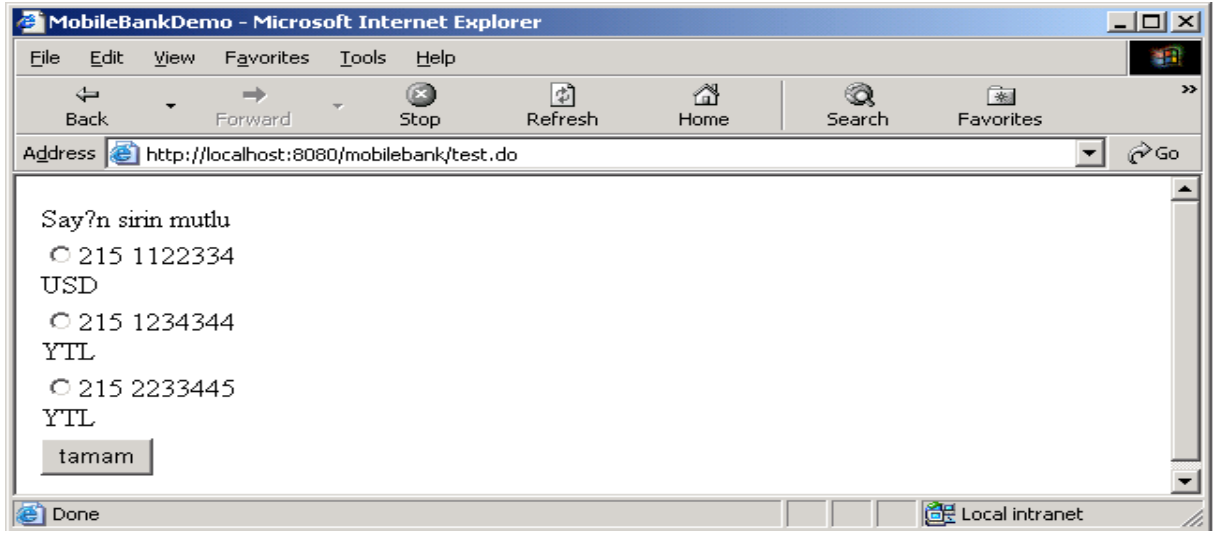


Main Menu :

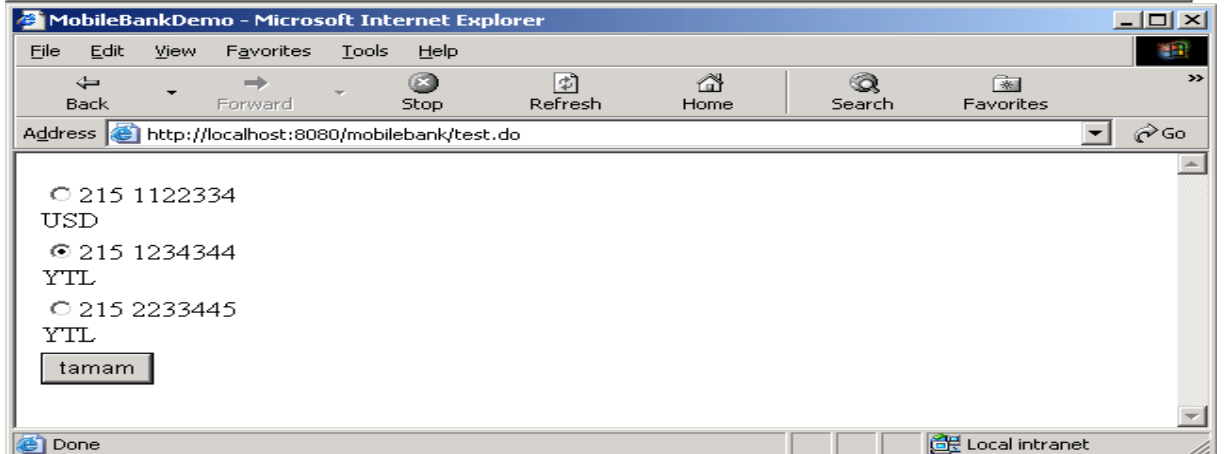
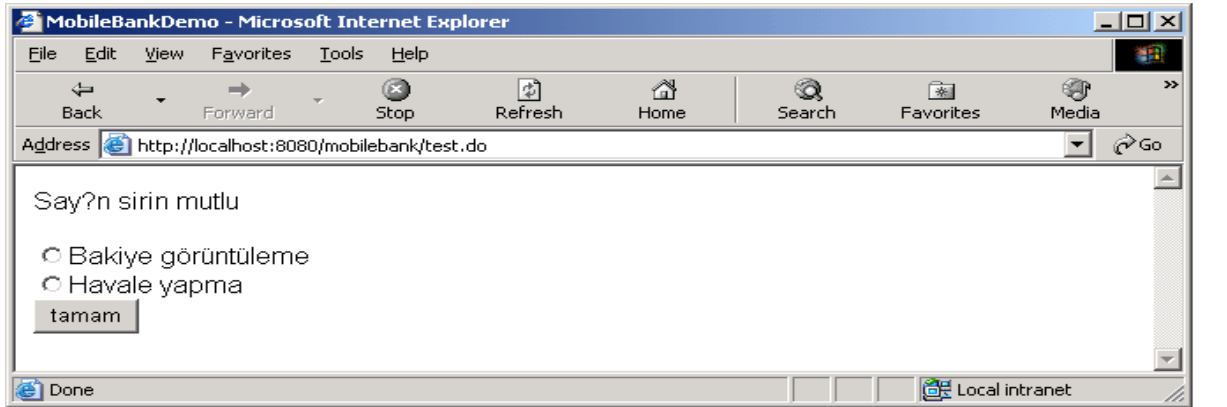


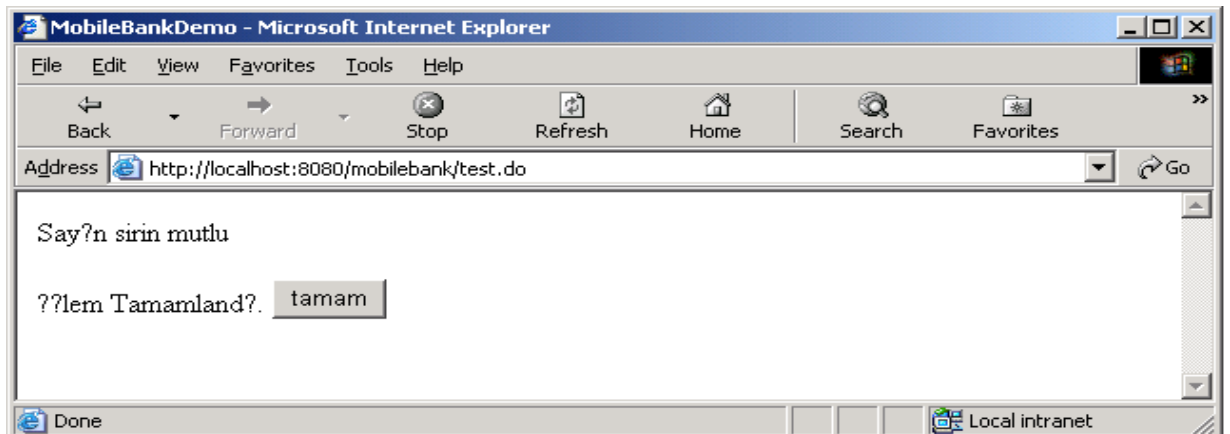
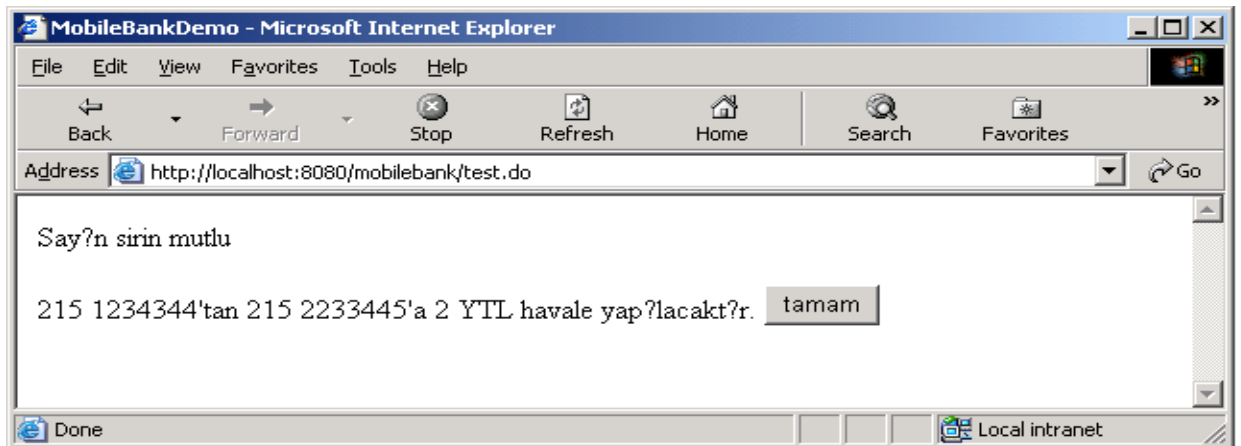
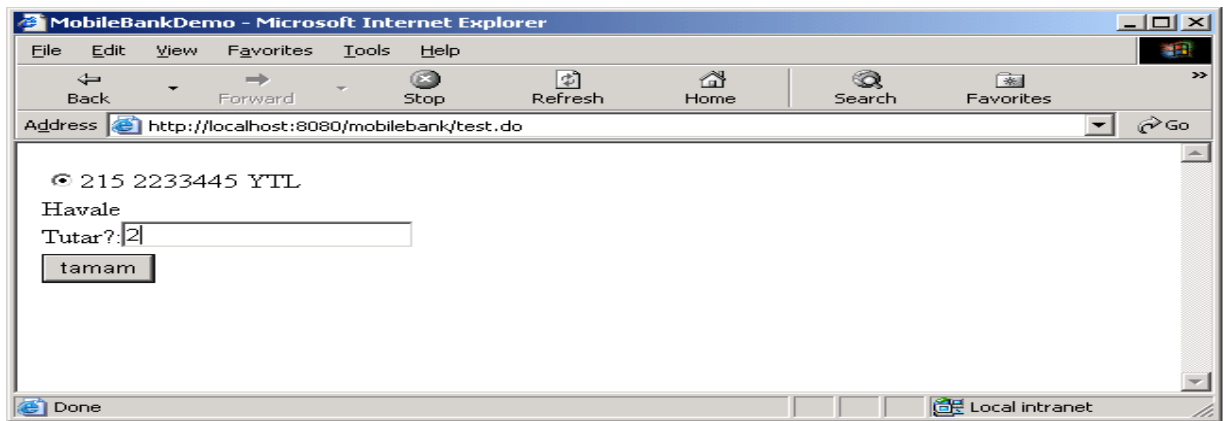
Bakiye Görüntüleme :





Havale Yapma :





IV. Software

1. Web Server

2. Database

3. Development Environment

1. Web Server

Apache Tomcat is the servlet container that is used in the official Reference Implementation for the Java Servlet and Java Server Pages technologies. The Java Servlet and JavaServer Pages specifications are developed by Sun under the Java Community Process. Apache Tomcat is developed in an open and participatory environment and released under the Apache Software License. Apache Tomcat is intended to be a collaboration of the best-of-breed developers from around the world.

Apache Tomcat is aimed at developers who will be using a text editor along with command line tools to develop and debug their applications. As such, the recommendations are fairly generic -- but you should easily be able to apply them in either a Windows-based or Unix-based development environment. If you are utilizing an Interactive Development Environment (IDE) tool, you will need to adapt the advice given here to the details of your particular environment.

Tomcat is aimed to run on JSK. It is an Interactive Development Environment for web application developer. To organize all the components of a web application, an actual directory and file hierarchy should be used to contain the source code of an application and others. These are some of the key tomcat directories:

- **/bin** - Startup, shutdown, and other scripts. The *.sh files (for Unix systems) are functional duplicates of the *.bat files (for Windows systems). Since the Win32 command-line lacks certain functionality, there are some additional files in here.
- **/conf** - Configuration files and related DTDs. The most important file in here is server.xml. It is the main configuration file for the container.
- **/logs** - Log files are here by default.
- **/webapps** - This is where your webapps go.

2. Database

PostgreSQL is an object-relational database management system (ORDBMS) based on POSTGRES, Version 4.2. POSTGRES pioneered many of the object-relational concepts now becoming available in some commercial databases. Traditional relational database management systems (RDBMS) support a data model consisting of a collection of named relations, containing attributes of a specific type. In current commercial systems, possible types include floating point numbers, integers, character strings, money, and dates. It is commonly recognized that this model is inadequate for future data processing applications. The relational model successfully replaced previous models in part because of its .Spartan simplicity.. However, as mentioned, this simplicity often makes the implementation of certain applications very difficult.

Postgres offers substantial additional power by incorporating the following additional concepts in such a way that users can easily extend the system:

- inheritance
- data types
- functions

Other features provide additional power and flexibility:

- constraints
- triggers
- rules
- transaction integrity

These features put Postgres into the category of databases referred to as *object-relational*. Note that this is distinct from those referred to as *object-oriented*, which in general are not as well suited to supporting the traditional relational database languages. So, although Postgres has some object-oriented features, it is firmly in the relational database world. In fact, some commercial databases have recently incorporated features pioneered by Postgres.

3. Development Enviroment

Altova XMLSpy® 2005 is the industry standard XML development environment for modeling, editing, debugging, and transforming all XML technologies, then automatically generating runtime code in multiple programming languages. XMLSpy® 2005 is the ultimate productivity enhancer for J2EE, .NET, Eclipse, and database developers that need the latest XML, Web services and database technologies.

In addition to its powerful XML modeling, editing, validation, and debugging capabilities, XMLSpy® 2005 supports the complementary technologies required to build the most advanced XML-based applications. Because XML documents must be bound to an external software application or runtime environment, XMLSpy® 2005 includes automatic code generation of Java, C++, or C# class files based on data elements defined in a schema.

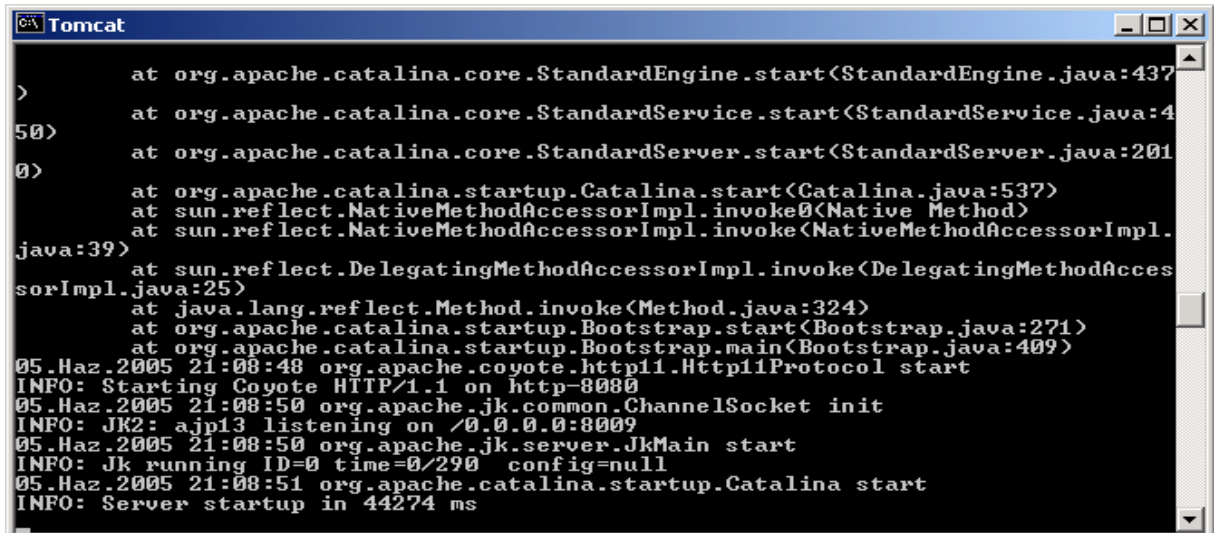
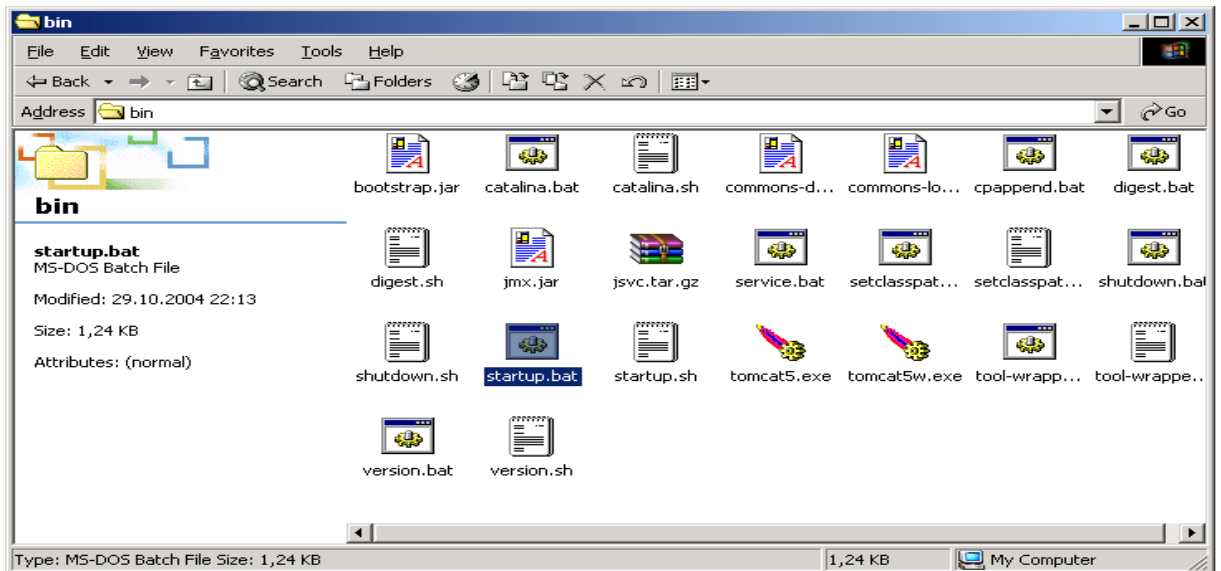
XMLSpy® 2005 lets you tackle Web services development on all of the major Web services platforms, including Microsoft .NET, J2EE, and Eclipse. Support for integration with Microsoft Visual Studio.NET and Eclipse allows you to seamlessly access the powerful XMLSpy® 2005 features from within these popular development environments. You can also access many of the powerful XMLSpy® 2005 functions in a programmatic way using the Java or COM systems integration API.

In addition, most advanced applications require interaction with relational databases, which house the majority of business information today. XMLSpy® 2005 supports the most popular relational databases in their native interface languages, allowing you to generate XML Schemas based on database structures, import and export database data, and generate relational database schemas from XML Schemas.

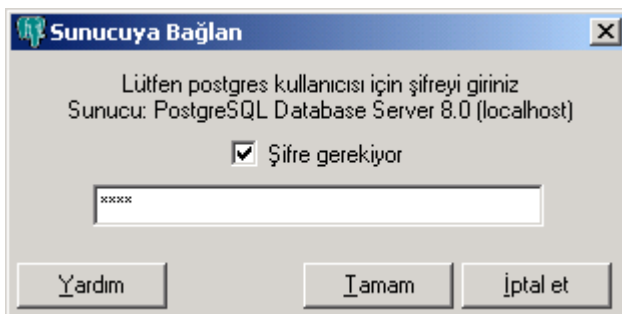
V. Requirements to Run the Application

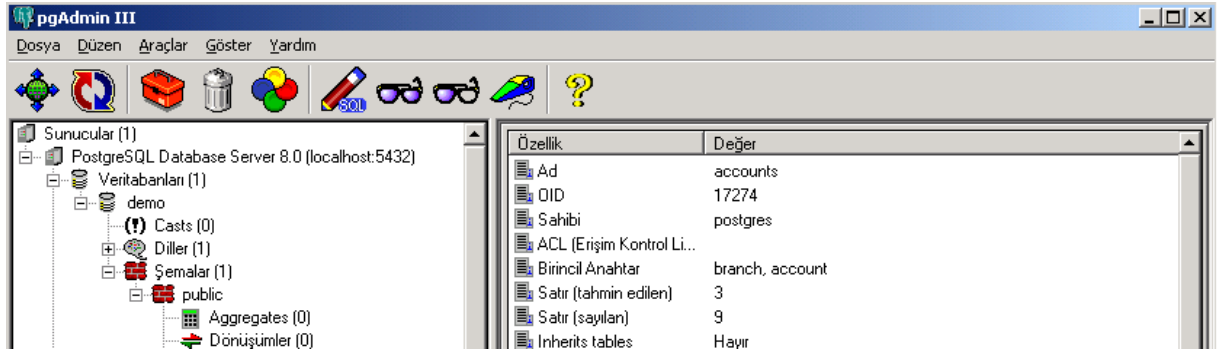
This application is run through web browser. To run this application you should start the following services in sequence.

1. Start TomCat :

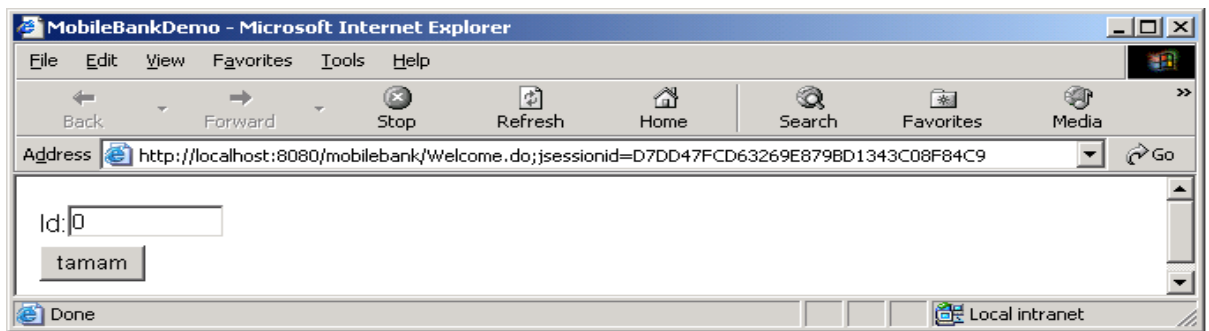


2. Connect to PostgreSQL Database Server:





3. Browse by using your internet explorer.



VI. Future Work

This implementation demonstrates only the two services from the whole Mobile Banking Application Service. And also it does not include any security mechanism at all. User interface is an xml page not a mobile phone for now.

As the real business model for Mobile Banking Application we will also have the below steps:

1. The device's physical form
2. The type of network
3. The Security Mechanisms
4. The Application Issues
 - 4.1. User interface :
 - 4.2. Menu structure
 - 4.3. Parameters and Messages
 - 4.4. Inputs
5. Application Components
6. Overview of Future Work

1. The device's physical form

The question is to find out which device will be the most successful to support mobile payments. The device can be a mobile phone or another such as a PDA, a laptop or any wireless enabled device that could process securely a financial transaction over a wireless network.

2. The type of network

With all the new wireless communication technology available, the choice of using one network technology over another is difficult. Each technology brings its own advantages and disadvantages. Therefore, the infrastructure should support the most suitable technology, depending upon the type of payment. Today, data communication networks (WLAN, Bluetooth, ...) and telephony networks (GSM, GPRS, UMTS, ...) bring a new dimension to the issue. In fact, telcos are confronted with WLAN technology that could be a real threat for their existing business. Some of the mobile network operators are already anticipating the potential success of this technology by offering hotspots.

3. The Security Mechanisms

Wireless communications present the obvious problem that even unauthorized parties can access the flow of sensitive data transmitted. There are already some methods that reduce the risk that unwanted people or devices intercept communication. Natural protections could simply come from the complexity of the protocol (i.e. frequency hopping). However, encryption is essential to secure the data. In order to use wireless PKI systems for mobile payment, improvements in device processing power and network bandwidth will have to be made.

4. The Application Issues

4.1. User interface :

4.2 . The menu structure will be like this:

Main Menu 1. My Accounts

Main Menu 2. Money Transfer

Leaf Menu 1: EFT

Leaf Menu 2: Transfer to my account

Leaf Menu 3: Transfer to another account

Main Menu 3. My Investments.

Leaf Menu 1: Buying Funds

Leaf Menu 2: Selling Funds

Main Menu 4. Credit Cards

Leaf Menu 1: Pay Credit Card

Main Menu 5. My Payments

Leaf Menu 1: Pay Bill

Main Menu 6. First Login

4.3. Parameters and Messages

Parameters and the message format will be as follows:

EFT

*EFT [accountnumber] [accountnumber] [requiredtime] [cost]

Transfer to my account

*TMA [accountnumber] [accountnumber] [requiredtime] [cost]

Transfer to another account

*TOA [accountnumber] [accountnumber] [requiredtime] [cost]

Buying Fund

*IHA [accountnumber][fundcode][fundtype][fundcount] [requiredtime] [cost]

Selling Fund

*IHS [accountnumber] [fundcode] [fundtype] [fundcount] [requiredtime]
[cost]

Pay Credit Card

*IKO [creditcardnumber] [creditcost] [accountnumber]

Pay Bill

*IFO [company] [date] [cost]**First Login :**

*ILK [ICCID]

4.4. Inputs

Numeric Inputs:

[**accountnumber**] : 0 - 11 numeric characters

[**creditcardnumber**] : 0 – 16 numeric characters

[**date**] : 6 numeric characters

[**fundcount**] : 0 – 16 numeric characters

[**cost**]: 0 - 13 numeric characters

Alphanumeric Inputs:

[**fundcode**] : 0 - 6 alphanumeric characters (A,B...,Y,Z; 0,1...,8,9)

[**creditcost**] : 0 - 13 alphanumeric characters ([T], [D], [A] or
numeric input 0,1,2,3,4,5,6,7,8,9)

Alphanumeric Inputs:

[**fundtype**] : 1 alphanumeric char. (E, Y, or space)

[**requiredtime**] : 1 alphanumeric char. (S, G, or space)

[**company**] : 20 alphanumeric characters

5. Application Components

Device

- basic (SIM, RFID, smartcard,...)
- dedicated (cellular, PDA,...)
- general (laptop,...)

Network

- operator-driven (GSM, UMTS,...)
- computer-based (WiFi,...)
- self-organized (Bluetooth, P2P,...)

Mobile Application

- presentation (WML, C-HTML, XHTML,...)
- communication (WAP, SMS, USSD,...)
- environment (J2ME, BREW, ME,...)

6. Overview of Future Work

Mobile Banking Service help customers to achieve banking transactions in an easy way secure way.

1. The id number is a unique number assigned per customer. In future work, telephone number may match with the account number.
2. The web browser makes the customer to access to the Mobile Bank transaction menus. In future work, *100# or *102# etc. makes the customer to access to the Mobile Bank transaction menus.
3. The required data can be entered using web browser as an XML application. In future work, the required data can be entered using the mobile handset. The user can browse other menus without payment.
4. The user is trusted site, he is not authenticated and authorized. In future work, if required, then the user can be authenticated and authorized by forcing to enter username and password.
5. Data send through XML, all tree site is simulated in one application. The user side, the telco operator side and the bank side communication is through this application. In future work, the smart SIM cards can help for identification, signing transactions, storing sensitive data and related service parameters. Also they facilitate displaying the approved data on the handset. The other security mechanism like encryption is also essential to secure the data. In order to use wireless PKI systems for mobile payment, improvements in device processing power and network bandwidth will have to be made.

Mobile bank service prototype has four key features:

6. Development of a special application that can be triggered by web browser.
7. Development of the structure for data communication between TELCO Application server and Bank web server.
8. Development of Web application according to the real Banking services.
9. Specifying customer information and account information format to be used for future work.

In future work, Mobile bank service will have five key features:

10. Development of a special applet that can be triggered by particular SMS.
11. Implement special security system on SIM. Thus the keys on SIM can encrypt the outgoing data and can be decrypted by the destination (Bank side only) only.
12. SMS message format between SIM to SMSC and SMSC to SIM
13. Development of USSD application or Web application by Bank.

14. Development of the protocol for data communication between TELCO Application server and Bank web server.

Reference number and Password are encrypted on the SIM with specific security algorithms and sent to the Bank web server over TELCO Application server which can decrypt the data with the particular keys.

The bank Application server performs the transaction after the verification of the password and the reference number.

To develop and test the USSD services a prototype is designed. For testing purposes a SMS-C server, an USSD server and an Application server is supposed to be used for the gateway between mobile user and the bank. . Mobile service is developed as USSD application.

VII. Conclusion

The biggest inhibitors in adoption of mobile banking services is the absence of on-line transaction based services with the offering that most of the banks have in their m-banking suite of products. Since more and more people are finding transactions through the Internet safer and faster, they would surely move to the SMS channel as the convenience is enhanced further on this channel.

This prototype has a purpose to give a general overview of Mobile banking. It aims to make this service more sensible and common. This is just a little part of the whole service. The whole service can be implemented in the way described during this report.

A BRIEF HISTORY OF LIFE

Şirin Mutlu Aktaş was born at January 15th, 1978 in Izmir. She was graduated from Izmir Kız Lisesi in 1995. Then, she moved to Ankara and studied at Computer Science & Engineering Department at Hacettepe University. Meanwhile she studied her English at Hertfordshire College in England for three months. After graduate, she went on METU for master degree at Information Engineering. After moving to Istanbul, she went on her master degree at Computer Engineering Department at Istanbul Technical University. Currently, she deals with network engineering as a main subject.