Abstract

Global mCommerce revenues are expected to grow from $400 million in 2000, to 22.2 billion by 2005. mCommerce is a key driver in developing the global information society, with applications emerging in numerous areas including banking, financial services, security services and shopping. With optimistic projections regarding its growth, many researchers are actively determining the future of mCommerce. In this paper, we have tried to synthesise some predictions and evolving definitions, explored security as a critical impediment and developing solutions; investigated the mPayment scenario; and derived a futuristic research framework. Specifically, we have attempted to capture the moving mCommerce scenario in present time, with a special focus into mPayments.

Introduction

With the rapid spread of mobile communication technologies, and parallel growth of Personal Digital Assistants, mCommerce is expected to become mainstream in many economies or rather globally. With approximately 1.7 million mobile connections, mCommerce was worth US20 billion in 2002 (NUA). If forecasts were to be true, mCommerce will reach an annual value of $13 billion or 7 percent of all eCommerce transactions (Mckinsey, 2000). Boston Consulting Group estimates that mCommerce will generate worldwide revenues of $100 billion by 2003, half of which will come from transactions from as many as 300 million users (Eftia, 2002). mCommerce is a key driver in developing the global information society, with applications emerging in numerous areas including banking, financial services, security services and shopping (Khalifa and Cheng, 2002).

With these optimistic projections, many researchers (see, Carlsson and Walden 2002; Dahlberg and Mallat 2002; Lehmann and Lehrer 2002; Vrechopoulos 2002) are in the process of defining mCommerce and determining its future. The literature in this area is still limited and evolving. There have been panels at world conferences addressing the issues in mCommerce across the world. The major focus of current research so far seems to be on technological constraints or innovations, lack of bandwidth, availability of devices and security. In this paper, we have tried to synthesise some predictions and evolving definitions, explored security as a critical impediment and developing solutions; investigated the mPayment scenario; and derived a futuristic research framework. Specifically, we have attempted to capture the moving mCommerce scenario in present time, with a special focus into mPayments.

1 Mobile commerce – where are we and where are we going - Panel Discussion at the 15th Bled eCommerce Conference, Slovenia.
defining mCommerce

As the mobile business itself is emerging, the definitions continue to evolve. Mcommerce is the selling of products and services via untethered devices such as palm top or mobile phone (1st eBusiness news, 2002). Paavalainen (2001:1) suggests that mobile business is “the exchange of goods, services and information using mobile technology”. For Kalakota and Whinston (1999; 2001) it is “…simply a way for improved customer interaction and new operational efficiencies, as it builds on all the investments in eBusiness”. Further, it is “an application infrastructure required to maintain business relationships and sell information, services and commodities by means of the mobile devices”

Keen and Mackintosh (2001) defined mCommerce as the “term for the extension of eCommerce from wired to wireless computers and telecommunications and from fixed locations to anytime, anywhere, and anyone” as it is becomes the part of new freedom economy. Kalevi Kontinen (2001)2 suggested that m stands for mobile and multi-modal ie wireless, anywhere and moving. Whichever definition is considered, they all seem to support the concepts of mobility, innovation and networked world. The key elements that emerge in research seem to be flexibility, value additions, convenient technologies that attribute to mobile commerce.

Methodological Framework

The main driver of our research is the relative lack of synthesized empirical documentation in the mCommerce area and the dynamic nature of the subject under study. Gavana et al (2001) recommended the exploratory investigation when there is relatively less information about particular situations or when there are no precedents available to extrapolate from. MCommerce research itself, being a new and evolving discipline, suited this method. Exploratory studies are crucial in getting insights into new phenomenon’s and for advancing knowledge using further methods.

The dynamic nature of the subject under study entailed an exploratory investigation, mainly through synthesized data collection from secondary sources. Jarvenpaa (1991) and Neuman (1997) endorse the method of synthesizing and analyzing data that has been collected for other purposes and making inferences for exploratory research in Information Systems Research. Further, being a current dynamic subject, most of the information is derived from conference presentations, white papers, panel reports, ongoing research working papers and few recent publications.

From the philosophical perspective, our research has taken a positivist or rather post-positivist critical realist approach. The positivist view is that the world is external and objective to the researchers; behaviors are explained on the basis of observable facts and preliminary inferences made from these observations (Ticehurst and Veal, 2000). The positivists essentially believe in discoverable reality through scientific empirical investigation (Blaikie, 1993).

However, our approach is leaning towards post-positivist critical realist philosophy (Trochim, 2002) which essentially suggests that there is a reality independent of our thinking or which science can study. Although, post-positivist critical realists also believe in empirical research

2 Senior VP Nokia Networks, Plenary address in ECIS 2001.
and inferences made by observation – the essential difference is that a ‘common sense’ based inductive reasoning method is used here, rather than conclusive deductive reasoning. The post-positivists also believe that all observations are fallible and therefore, the results of any investigation may need revision from time to time. Given the dynamic nature of this topic, this philosophical approach suited our research focus, with a futuristic framework.

Global mcommerce

Based on mobile growth connections, mCommerce revenues are forecast to grow exponentially. According to Jupiter research, global mCommerce revenues will grow from $400 million in 2000, to 22.2 billion by 2005 (Raczkowski, 2002). Table 1 indicates the worldwide mCommerce revenue predictions, derived from a survey conducted by AT Kearney.

Table 1: World Wide Mobile Commerce Revenues 2000-2005 (in billions)

<table>
<thead>
<tr>
<th>Region</th>
<th>2000</th>
<th>2001</th>
<th>2002</th>
<th>2003</th>
<th>2004</th>
<th>2005</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia</td>
<td>$0.4</td>
<td>$1.3</td>
<td>$2.6</td>
<td>$5.0</td>
<td>$7.4</td>
<td>$9.4</td>
</tr>
<tr>
<td>Latin America</td>
<td>$0.0</td>
<td>$0.0</td>
<td>$0.0</td>
<td>$0.1</td>
<td>$0.2</td>
<td>$0.5</td>
</tr>
<tr>
<td>North America</td>
<td>$0.0</td>
<td>$0.1</td>
<td>$0.2</td>
<td>$0.7</td>
<td>$1.8</td>
<td>$3.5</td>
</tr>
<tr>
<td>Western Europe</td>
<td>$0.0</td>
<td>$0.1</td>
<td>$0.5</td>
<td>$1.7</td>
<td>$4.6</td>
<td>$7.8</td>
</tr>
<tr>
<td>Rest of the World</td>
<td>$0.0</td>
<td>$0.0</td>
<td>$0.1</td>
<td>$0.2</td>
<td>$0.4</td>
<td>$1.0</td>
</tr>
<tr>
<td>Total</td>
<td>$0.4</td>
<td>$1.5</td>
<td>$3.4</td>
<td>$7.7</td>
<td>$14.4</td>
<td>$22.2</td>
</tr>
</tbody>
</table>

Research seems to suggest that Europe is moving rapidly towards mCommerce with rapid growth of the Global System for Mobile communication (GSM) and service extensions (HSCSD, GPRS, EDGE). However, as the findings of one research panel suggests, business cases were calculated rather too soon, with extreme expectations. The auctions for UMTS frequency band packages will necessitate high pricing levels. In conjunction with the market fall in international telecom stocks since mid 2001, some countries in Europe have dropped well behind expectations and further, GPRS itself have been slow in diffusion⁴ Nevertheless, the market for mCommerce in Europe alone is estimated to be worth Euro 3 billion by 2003 (KPMG 2000, Muller-Veerse 1999) and expected to touch $7.8 billion by 2005, in Western Europe alone (Raczkowski, 2002).

In the Asia Pacific Region, with the exception of Japan⁴, delay in the launch of higher bandwidth and infrastructure in addition to ‘culture specific’ barriers seem to impede mCommerce growth – especially in economies such as Korea. Interestingly, the mobile phone and Internet have not converged in this country, as the phone is still an audio device only. In China, bad debt and WTO entrance commitments seem to be the issue. Hongkong and Singapore seem to have high potential in mobile shopping and banking (Carlsson and Walden, 2002). According to Jupiter research (Raczkowski 2002), Asia is expected to lead with $9.4 billion in mCommerce revenues by 2005. Interestingly, developing economies in Asia, such as India have high potential for mCommerce with high acceptance ratios. Although there are security concerns, the convenience offered by mCommerce seem to be a key acceptance factor, especially in regions with high levels of business population. The

---

⁴ Mobile commerce – where are we and where are we going - Panel Discussion at the 19th Bled e-Commerce Conference, Slovenia.
⁵ Japan's i-mode users spend US$21.60 a month (mCommerce world 2001).
availability of indigenous PDAs and mobile devices also has accentuated the diffusion of mCommerce.

In the US, mCommerce is maturing while the popularity remains questionable. According to Forbath and Neff (2001) business applications with clear value propositions are likely to lead the way. These may include: wireless extensions of logistics, sales force automation, customer relationship management, field service and support functions. MCommerce revenues are expected to reach $3.3 billion in US (Raczkowski, 2002). Durlacher claims that the UK alone will generate £2.1bn from mCommerce in 2003 (Dti Telewest 2002). Wireless World Forum (2002) predicts that Japan, USA, Germany and UK will represent four of the largest mobile payment markets in the world by 2006 and forecasts more than 200 million regular mobile payment users, spending a total of 47.2 billion Euros.

Security – a Crucial Impediment

Security is perhaps a top concern in the untethered world, as consumers move from PCs to PDAs (Emmerson 2001) and many claim that this concern is impeding the growth of mCommerce to a large extent (see Ding and Unnithan 2002). However, Hampe et al (2001) disputed the security concern on mobile devices by arguing that digital mobile phone networks are encrypted, which ensures that messages cannot be added, deleted or modified. Therefore, the sole ownership characteristic of the mobile phone supports non-repudiation of transactions by customers, thus safeguarding the vendors. However, as Kalakota and Robinson 2001; Ghosh and Swaminatha 2001) point out, the full potential of consumer and business applications cannot be realised unless there is sufficient level of trust in the underlying security of mobile networks and end-to-end security provision is available.

The primary goal of security in mCommerce is to ensure privacy, data integrity and authentication between the user and the vendor or organisational system. Key features for highly secure mobile commerce (Singh 2002; Paavilainen 2001; Sonera Smart Trust 2001, Torvinen 2000, Engel-Flechsig 2001) include authentication, non-repudiation, encryption, data integrity and confidentiality (see Ding and Unnithan 2002 for detail). According to Jormalainen and Laine (2000) the acceptable and sufficient level of security is a compromise between the usability and strength of the used encryption method. The Digital Signature Law passed in the late nineties/early 2000 saw the introduction of a statutory requirement for asymmetric encryption, where both parties involved has a pair of keys, i.e. a public and a private key. Member countries of European Union, Americas, most Asian and Asia-Pacific countries already have legislation on electronic signatures - which offers a solid foundation upon which the business world can build a solid eCommerce structure (Sievers 2000b).

As mobile devices are location-independent, personal, portable and widely distributed, they are well suited to become one of the dominant enablers for carrying out financial transactions electronically (Torvinen 2000, Muller-Veerse 1999), but, due to their mobile nature, notebook PC and wireless communication devices are more susceptible to security risks (Intel 2001). While banks in Europe are investing heavily in mobile banking; all major banks in Scandinavia are offering wireless services, accounting for 48 percent of total Western Europe’s WAP-enabled mobile banking accounts, with 22 percent in the UK and 13 percent in Germany (Engel-Flechsig 2001). However, the customers in the USA are still sceptical of mobile banking due to perceived security risks (Keen and Mackintosh 2001). A survey highlighted that more than 70 percent of wireless users in the United States and Canada have concerns and privacy of their wireless communications (Mayor 2001b). It is apparent that
mCommerce will only reach its full worldwide potential when confidentiality, authentication and non-repudiation can be guaranteed for online transactions (Kalakota and Robinson 2001; Lannerstrom 2000). Applications like wireless banking are only limited to ‘information provision’ or read only as the mobile security still lacks the ability to conduct a legally binding transaction (Mayne 2001).

Security breaches associated with wireless networks include interception of data such as credit card authorization and law enforcement data, email messages, stealing of cellular airtime and physical breach of security at unmanned base stations or other communication centers (Chen 2001). Currently, no mobile network operator can guarantee that confidential information (e.g. credit card details, personal information trade secrets, or business documents) can be transmitted over the mobile net securely. Therefore trust has to be built into the wireless environments (Torvinen 2000). mCommerce also faces many more privacy and security risks such as the nature of the medium, required trust and cooperation between member nodes within the network, which can be exploited by malicious entities to deny service as well as to collect confidential information, and disseminate false information. Additionally, the devices and Wireless Markup Language (WML) language developed for wireless devices have failed to adopt fundamental security concepts employed in the current generation of desktop machines (Paavilainen 2001; Kalakota and Robinson 2001).

Manufacturers of many wireless devices have failed to include basic operating systems security features to protect access to the memory. This is a risk as rogue applications can “steal” decrypted data (e.g. private key) by interrupting it at the right moment. Thus becoming a weak link in the converged data world as open standards bring unlimited possibilities for the propagation of malicious code (Ghosh & Swaminatha 2001, Durlacher 2001). NTT DoCoMo’s introduction of JAVA service for mobile phones resulted in an emergence of Trojans viruses that could cause the handsets to place calls to a large number of people or dial an emergency number (Durlacher 2001, Mobilecommerceworld 2001).

Additionally, the lack of access control for WML script means that rogue WML script can be pushed to a device without the owner’s knowledge (Schuba & Wrona 2001). The potential damage can range from exposure of personal identifying information that is kept on the device to the exposure of credit card details, banking account details, user name and passwords associated with these accounts via the use of bogus web sites. Malicious scripts will then have the ability to falsely ring up charges or potentially divest money from smartcards or bank accounts (Paavilainen 2001). Therefore, the most significant risk to mobile commerce systems will be from malicious code that is beginning to penetrate the wireless network. It also has the ability to undermine other security technologies such as signing, authentication and encryption (Ghosh & Swaminatha 2001; Schuba & Wrona 2001).

Wireless devices pass through many different, potentially non-trustworthy networks from which service is derived and data is exchanged. Information can be stolen or altered without the end users knowledge. Most vendor implementations of Secure Socket Layer (SSL) or Wireless Transport Layer Security (WTLS) do not reauthenticate principals or recheck certificates once a disrupted service is re-connected. Attackers can use this vulnerability to their advantage (Ghosh and Swaminatha 2001, Lubinski 1998). Dramatic drops in hardware prices during 2000-2001 have made it attractive and convenient for corporations and home user to go wireless, in particular with equipment built on the IEEE 802.11b standard (Kalakota and Robinson 2001). But computer security experts say that in the rush towards liberation from the tethers of computer cable, individuals and companies are opening the
doors to a whole new type of computer intrusion. Hardware to listen to 802.11 transmissions is readily available to attackers in the form of consumer products (Poulsen 2001) such as Windows XP.

Security Technologies

The SSL protocol maintains the security and integrity of the transmission channel by using encryption, authentication and message authentication codes. Mobile security technology emerged in the form of Secure Socket Layer (SSL) within a closed end-to-end system with GSM phones. The smartcard within the terminal, the SIM (Subscriber Identification Module) card, provides authentication of the owner and enables a higher level of security than typically achieved in the fixed Internet environment. Paavilainen (2001) pointed out that Nordea, Nokia and Visa are developing electronic mobile payment services that enable secure mobile payments through dual-slot mobile phone with chip cards i.e. the first slot is the SIM card that identifies the consumer, and the second is for a small credit card, which enables variety of transactions from vending machines to supermarket purchases (Paavilainen, 2001).

Wireless Public Key Infrastructure (PKI) system is a comprehensive security system that is based on three elements: two encryption keys, a digital signature, and a security certificate. The weakness in PKI is that there must be a third party organisation, called the certificate authority, which keeps and catalogs the public keys of the sender and the receiver. Secure transactions with strong PKI encryption can be done using a special SIM card inserted into a mobile phone (Paavilainen 2001). However, in spite of the advantages of a public key cryptosystems, it is not fully utilized because of the poor computing power and small battery capacity of a mobile phone.

The Wireless Application Protocol (WAP) was developed by the WAP Forum industry association to provide specifications for the applications that operate over wireless communication networks (Jormalainen and Laine, 2000). WTLS is a layer that operates above the transport protocol layer and it provides the upper level layer of the WAP with a security transport service interface. It is the first attempt to provide a secure end-to-end connection for the WAP. To achieve maximum level security, the WAP gateway must reside on the local network as the content server. However, none of the commercially available WAP Gateways actually implements the security protocol and there is no security in today’s WAP applications with existing products (Brooks & Warren 2001, Scuba & Wrona 2001; Chan 2000). There is a debate regarding the “WAP Gap” where there is a lack of security at the point when wireless request to web pages are translated at the WAP gateway from the WTLS to the standard SSL protocol used in securing HTTP requests. Perpetrators are able to compromise the message at this point of transfer when data is not protected by either the WTLS or SSL security technology (Ghosh and Swaminatha 2001; Chan 2000; The WirelessFAQ 2001).

Wired Equivalent Privacy is a security protocol for wireless local area networks or WLANs defined in the IEEE 802.11b standard, designed to provide the same level of security as a wired local area network. However, WLANs, which utilise radio waves, do not have the same physical structure and therefore are more vulnerable to tampering (Webopedia, 2002). WEP is part of the system security of 802.11 and its goals are to provide confidentiality and data integrity, and to protect access to the network infrastructure by rejecting all non-WEP packets (Loeb 2001). WEP aims to provide security by encrypting data over radio waves so that it is
protected as it is transmitted from one end point to another by using a secret key shared between the communicators. However, radio waves can extend outside the organisation's physical premises and are receivable from a distance (Issac 2001). Someone can passively retrieve sensitive information from a distance without being noticed by network security personnel (Durlacher 2001; Weatherspoon 2000; IBM Research 2001). In the year 2001, several scientists managed to read WEP-protected traffic, add bogus traffic into a WEP-protected network as well as change WEP-protected traffic in transit. This flaw in WEP prevents it from providing even a minimal reliable level of security for serious applications.

Security continues to be a major issue. Although, industry players and trade consortiums are endeavouring to formulate an environment that allows mobile operators, financial institutions and other service providers to facilitate secure mobile transactions, a secure end-to-end security has not been provided to address all security concerns as yet (Ding and Unnithan 2002).

**Mobile Payments**

Kruger (2001) defined mPayments as payments via the mobile phone. Heijden (2002) identified a definition in line with the Shon and Swatman (1997) definition of an internet payment system ie any conventional or new payment system which enables financial transactions to be made securely from one organisation or individual over a mobile network. Some experts believe that the mobile phone will even replace smart cards as a means of payment (Kruger 2001, Henkel and Zimmermann 2001, Bucci 2001) as they have an embedded chip that may be used to store value or secure authorisation. If mass-market mCommerce diffusion has to be achieved, a successful mPayment system needs to be developed (KPMG 2000; Henkel & Zimmermann 2001; Kruger 2001). By 2005 the number of US based mPayment users are expected to rise to 3.5 million, making the mPayment system a critical hub in the bank/consumer relationship (TowerGroup 2001). Forrester Research claims that the mobile payment market will be worth $22 billion by 2005 - making it the fastest growing part of the global payment scenario (Baschnonga 2002). Compared to other payment systems, mobile payments have the particular advantage that they can be used at the real point-of-sale, as well as in eCommerce and in mCommerce (Krueger 2001, Dahlström 2001).

Mobile Payment is a point-of-sale (POS) payment made through a mobile device, such as a cellular telephone, a smart phone, or a personal digital assistant (PDA). Using the mPayment method, a person with a wireless device could pay for items in a store or settle a restaurant bill without interacting with any staff member. This ability makes it a potential eCommerce and mCommerce application. (Krueger 2001). Mobile payments are used to pay not only for merchandise purchased via mobile channels but also for transactions in the physical world such as vending machines, passport photo machines, car wash machines etc (Paavalainen 2001). mPayment is already in use in many parts of the world, including Europe and Asia - even though not of large significant as yet. There are several providers offering mPayment systems services although the predominant players are Telcos and Financial institutions (what is.com, MeT 2001, Krueger 2001b, KPMG 2000, Bucci 2001). Table 2 provides some examples of mPayment systems as of December 2001 (Krueger 2001). The highlights are where mobile operators are participating in the mPayment ventures.
Table 2  mPayment Ventures

<table>
<thead>
<tr>
<th>SUPPLIER</th>
<th>TYPE OF TRANSACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banko maxi (Austria)</td>
<td>Virtual POS</td>
</tr>
<tr>
<td>Bibit (Holland, International)</td>
<td>Mcommerce (WAP Enabled)</td>
</tr>
<tr>
<td>Cellnet (Sweden, Netherlands)</td>
<td>Parking</td>
</tr>
<tr>
<td>Cingular Direct Bill (USA)</td>
<td>Virtual POS</td>
</tr>
<tr>
<td>EMT (Estonia)</td>
<td>Parking</td>
</tr>
<tr>
<td>GiSMo (Sweden, UKL, Germany)</td>
<td>Virtual POS</td>
</tr>
<tr>
<td>Metax (Denmark)</td>
<td>Real POS (filling stations)</td>
</tr>
<tr>
<td>Mint (Sweden)</td>
<td>Real POS</td>
</tr>
<tr>
<td>NTT DoCoMo (Japan)</td>
<td>MCommerce (subscription)</td>
</tr>
<tr>
<td>Omnitel Onphone (Italy)</td>
<td>Virtual POS</td>
</tr>
<tr>
<td>Orange Mobile Payment (Denmark)</td>
<td>Payment for prepaid and invoice</td>
</tr>
<tr>
<td>Oskar (Czech Republic)</td>
<td>Mail order and virtual POS</td>
</tr>
<tr>
<td>Paiement CB sur mobile (France)</td>
<td>Real and virtual POS</td>
</tr>
<tr>
<td>Paybox (Germany, International)</td>
<td>Virtual POS, P2P</td>
</tr>
<tr>
<td>PayDirect (USA)</td>
<td>Virtual POS</td>
</tr>
<tr>
<td>PayPal (Germany)</td>
<td>Virtual POS</td>
</tr>
<tr>
<td>Payline (France)</td>
<td>Virtual POS</td>
</tr>
<tr>
<td>PayPal USA</td>
<td>Virtual POS, P2P</td>
</tr>
<tr>
<td>Phone Paid UK</td>
<td>Real POS (incl vending machine)</td>
</tr>
<tr>
<td>Sonera Mobile Pay (Finland, Sweden)</td>
<td>Real and Virtual POS</td>
</tr>
<tr>
<td>SteelCash (Germany)</td>
<td>Tickets</td>
</tr>
<tr>
<td>Telenor Mobil (Norway)</td>
<td>Virtual POS</td>
</tr>
<tr>
<td>Telia Pavit (Sweden)</td>
<td>Real and Virtual POS</td>
</tr>
<tr>
<td>Visa Movil (Spain)</td>
<td></td>
</tr>
</tbody>
</table>

Source: Krueger 2001

Korea's Seongnam City, south of Seoul, piloted a mobile payment system “Zoop” which connect the city's stores to a central payment system via broadband links. The mobile payment system runs on infrared technology and will be used for transit payments, for goods and services at retail locations and in restaurants around the city (Korean Herald 2002). The Finnish carrier, Sonera, is running a mobile payment trial in Helsinki, with Visa- and Eurocards (MasterCard's) complementing its prepaid Shopper service, to which funds are transferred from users' bank accounts. Payments in the pilot are added to the customer's credit card invoice, or debited to a Shopper account (Cnet 2002). In Australia, Telstra Mobile and the City of Melbourne have commenced a three-month mCommerce parking meter trial in September 2002, where customers can elect to pay for their parking via their eligible mobile phone or cash (Telstra 2002). Coca-Cola and Telstra have partnered to bring in the Dial-a-Coke service in Australia. The mobile phone users in Australia can now use the phone to buy and the cost of the bottle will appear in the next mobile bill (Telstra 2002). In Germany, IBM (NYSE:IBM) Global Services and leading international mPayment provider, paybox.net AG, have announced a joint initiative to drive mCommerce through an integration of systems and an expansion of services which includes wireless vending machine payments and retail point-of-purchase solutions.

Baschnonga (2002) points out that Paybox is one of the most successful mobile payment services to date. Paybox is available in the UK, Germany, Sweden, Austria and Spain and ignores the mobile Internet and PKI, instead relying on just a four digit PIN in addition to the customer's mobile number. In this way it works with any terminal and on any network - a level of convenience that has allowed the company to steal an early march on other European competitors. Backed by investor Deutsche Bank and working with retailers, Paybox teamed
up with US-based PayStar in February 2001 in order to launch a 'PizzaFone' service with an
as yet unnamed national Pizza franchise where orders are paid for on delivery using a
cellphone (Baschnonga 2002). Bucci (2001) highlighted that the Italian banking institutions
believe that providing mobile payment services to their customers are their first priorities.
TIM (Telecom Italia Mobile) who has jointly developed a system with Oberthur Card
Systems and Societa' per i Servizi Bancari (SSB), that allows the mobile phone user to carry
out banking functions and mPayments. TIM and Banca Popolare di Milano (BPM) have
jointly launched We@TIM, a set of services for on-line trading, mobile banking and
generalised access to eCommerce.

Omnitel has launched a trading service along with Self Trade, a French broker on the Net.
Issues in mPayments include standardisation and security. Standardised mobile payment
systems are a pre-requisite for the wide scale adoption of mCommerce service (Hampe and
Swatman, 2001) A host of different solutions have been proposed to enable mobile payments,
leading to a need for standardization, which may be reached by regulation, voluntary
agreements, or market forces (Henkel and Zimmermann 2001, Krueger 2001b). Interoperability is central to the move towards next-generation networks and the effective
functioning of mobile payments will require cooperation and interoperability (Krueger
2001b, MeT 2001).

Several initiatives are underway to provide ubiquity of services either by a centralized
solution or by cooperative solution. Early this year, two existing bodies, the WAP Forum and
the Open Mobile Architecture, have been dissolved to form the Open Mobile Alliance
(OMA) as the first steps towards wireless technology unification in its bid to devise open,
interoperable standards industry needs to bridge the gaps among all the players (Open Mobile
Alliance 2002). A consortium of companies called PayCircle, including Sun Microsystems
Inc., Hewlett-Packard Co. and Oracle Corp., Lucent Technologies and Siemens AG and
several other smaller companies have teamed to create standards for the way transactions
originating on mobile devices are handled (Costello 2002). PayCircle will attempt to correct
non standardization by creating standard interfaces by which payment systems, wireless
networks and vendors will be able to communicate (Costello 2002).

In Europe, the European Committee for Banking Standards (ECBS) and the European
Telecommunications Standards Institute (ETSI) has signed a co-operation agreement to
increase the effectiveness of their efforts towards the development of standards for the
security of telecommunications and m-commerce (mTravel.com 2002). RichSolutions is
offering a mobile applications suite, RichPayments for Mobile Devices, to render PDAs and
mobile phones as mobile credit card terminals that support signature capture and receipt
retrieval. Visa International announced a new global specification that ensures the security of
Internet payments made over mobile phones. The Mobile 3-D Secure specification is based
on existing payment technologies and extends payment authentication initiatives, enabling
Visa card issuers to validate the identity of their cardholders in real time (Visa 2002).

Conclusion and Further Research

It is evident that mCommerce is here to stay and evolve. The breadth of mCommerce will
continue to change and definitions will emerge. Secure and standard technologies, network
and mPayment methods seem to dominate the mCommerce impediments. Industry
consortiums together with economic forums are continually trying to address these issues in
various forums, involving many economic forums, mobile operators and also financial
institutions, if mCommerce has to be diffused into the mass-market. Improvement of security technologies and legal framework continues to be high on the agenda of developers, vendors as well as various consortiums.

In this context it is crucial to define standards now, as to guarantee real mobility so that mCommerce applications will be usable across borders and independent from the current mobile infrastructure. In addition, there are necessary amendments to other areas such as banking laws and retail traditions. We hope to see a significant change in the way mobile devices are used, with a chance to replace not only the mobile phone but also the wallet, CD player etc.

This research is a vision in time – and highlights some major issues that concern mCommerce globally and initiatives in various economies, especially in relation to mobile payment issues. It also provides some existing and predicted figures for the growth of mCommerce in different economies. Future research may address specific economy concerns, technological issues, economic factors that influence mCommerce, etc. Cross-economy comparisons and longitudinal studies may bring forth richer and much more in-depth results, on which lawmakers, consortiums and developers can build upon.

When looking at mobile devices it is also necessary to deal with restrictions of those devices. Therefore we have had a look into software technical aspects of mobile devices, especially PDAs (Fraunholz and Jung 2002). We are currently working on a framework for mobile software development to provide fast and reliable artefacts. Additionally, we aim to build a framework for the consolidation of mCommerce research from the patterns available and develop futuristic strategies for the benefit of academia and researchers, as well as industry consortiums. This framework will involve all factors that may influence mCommerce extrapolated from the current views and the consolidation of the research.

References


Bucci, P (2001) Mobile Financial services and m-Payments in Italy URL: http://epso.jrc.es/newsletter/vol01/1-4.html; Accessed: 10/08/02
22.140_8000_1104595457&return=y&site=ehost, Accessed 12/10/2001