

Electronic Commerce Transactions in a Mobile Computing Environment

Prof. Jari Veijalainenⁱ and Prof. Aphrodite Tsalgatiidouⁱⁱ

Abstract-- Internet E-Commerce has been flourishing for the last few years, especially with the advent of world wide web. Mobile Electronic Commerce has started recently to appear in the scene by exploiting the advantages of internet, mobile computing and mobile communications in order to provide a large number of advanced services to mobile users. The potentials of mobile e-commerce are enormous while related technical, business and legal issues become more complicated. The goal of this paper is to present and discuss problems associated with the trading and billing of tangible and intangible goods in an environment, where mobile handheld devices are used to conduct transactions and to identify requirements for these.

Index Terms-- Transaction Processing, Mobile Electronic Commerce, Mobile Computing, Wireless Application Protocol, Wireless Networks

I. INTRODUCTION

Electronic Commerce (E-Commerce, EC) concerns the digitization of markets and the emergence of a new industry to sustain these electronic markets. The last few years, with the advent of World Wide Web there has been a remarkable growth in the business to consumer E-commerce (B-to-C EC) which to a great extent is synonymous with electronic retailing. A large number of shopping opportunities all over the Internet appeared the last few years offering every kind of goods from digital audio and video (mp3, real-audio etc.) to physical books and CDs, and lately even to cars and houses (see e.g. Amazon's site [22]).

Mobile Electronic Commerce (MEC) has started recently to appear in the scene as a result of the continuously increasing number of hand-held devices, which makes them an ideal channel for offering a large number of advanced services to mobile users by exploiting the advantages of Internet, mobile computing and mobile communications. As MEC we define any type of economic activity that is considered as electronic commerce by legislation of some country or by business community *and* that is performed using a mobile wireless terminal by at least one party. In most cases the mobile terminal is used by a customer (not

by merchant or bank) and the wireless network used is a wireless telecommunications network, although any other wireless network, such as wireless IP network could be used, too.

We are aware that the definition of MEC above is still vague and raises many questions. One reason is that the very concept of electronic commerce is currently not very precisely and uniquely laid down. Second, the concept of mobile computing is also still evolving; some people have coined the term ubiquitous computing to address the possibilities of anywhere, anytime computing. Mobility does not preclude mobile devices, but in our view the new possibilities and challenges for the EC are brought up via wireless portable terminals that are typically personal and hand-held.

Our view is thus that MEC is a special case of EC, i.e. MEC has all the opportunities and problems that EC has, but it offers in addition some novel and very exciting possibilities - as well as new threats and challenges. Technical, business and legal issues become more complicated in MEC than in EC performed using stationary workstations and similar devices.

A number of MEC-specific novel applications and services, especially localised and personalised services have started to appear. We consider the location-based services now emerging in 2G+ and 3G telecommunication networks to fall under MEC in this context. At the same time, applications and services already offered in Internet for PC level fixed terminals are becoming available for mobile users. Thus, users can now buy various things, order goods and services, etc. using their mobile hand-held terminals instead of PCs. Although there are still differences between the quality and variety of services for different terminal types, they are becoming smaller, even vanishing.

The Wireless Application Protocol (WAP) [14] plays an important role in especially GSM-based MEC as it bridges the gap between the mobile world and the Internet world (TCP/IP networks) by optimizing standards for the unique constraints of the wireless environment. It also offers complicated enough security mechanisms and application platform for mobile electronic commerce applications to be developed.

The goal of this paper is to present and discuss problems associated with the trading and billing of tangible and

UNIVERSITY OF JYVÄSKYLÄ, Department of Computer Science and Information Systems, Agora Building, PO Box 35, FIN-40351 Jyväskylä.
E-mail: jari.veijalainen@jyu.fi, afrodite@jyu.fi

intangible goods in a mobile computing environment and identify their transactional and other requirements. It is organized as follows: section 2 describes the steps and activities of the trading and billing process and the problems and critical issues associated with it. The issue of mobility and its effect in the e-commerce processes and transactions is examined in section 3, while section 4 discusses transactional requirements for a mobile e-commerce environment and finally section 5 concludes the paper.

II. THE TRADING AND PRICING PROCESS IN BUSINESS TO CONSUMER E-COMMERCE AND MOBILE E-COMMERCE AND RELATED LEGAL ISSUES

A. General form of the trading process

The main phases of the trading process derived from a set of studies (e.g. [8, 7] and from the Electronic Commerce Directive [3] are:

- Information acquisition: during this phase the customer acquires information about merchants and products offered over the Internet and evaluates them. Intermediaries can add value in this process by providing for example product comparisons.
- Negotiation: during this phase, the customer and the seller negotiate the terms of the contract regarding mainly the method of payment and the method of shipping. The negotiation phase may have different forms. In business to consumer (B-to-C) electronic commerce, negotiation begins with the direct contact between the customer and the merchant (e.g., banner-ad leading to the homepage of the merchant showing the product characteristics and price). The customer can continue the negotiation by bargaining, selecting the goods, the method of payment and delivery. The negotiation ends when an order is placed and all details confirmed, including all costs.

Currently, the negotiation is rarely possible towards the merchants; the customer has to accept the prices and conditions laid down at the site, or choose another site. The situation might, however, change in the future when more advanced technology is applied.

- Execution phase: the customer and merchant have reached an agreement, and both have to meet the obligations of the contract established during the negotiation phase. Thus, the customer has to fulfill his payment obligations and the merchant has to deliver the goods. Each merchant can have its own policy regarding delivery of goods before or after receiving the payment; this can be defined in the contract.

- After-sales phase: This is often forgotten from the considerations, but in reality it has often much meaning to the customer. If the customer is not satisfied with the product, she can return it within a certain period of time after getting it or require lower price, etc. Also if the product is somehow broken, the customer can get it fixed or replaced on the cost of the merchant or manufacturer based on the granted guarantee.

B. Dispute Handling And Other Related Legal And Technical Problems during the after sales phase

If everything runs smoothly, the process is terminated after a successful completion of the first three steps of the 'Execution phase'. Disputes may arise in many cases: the delivery may not correspond to the order, product may be defect upon reception or becomes soon defect, payment could not be settled, ordering process might not conform to the regulations, the ordering transaction could not be made legitimate, or it may be repudiated. As merchants can reside physically anywhere on earth, settling and disputing can become very costly to customers. This can also create an opportunity for speculation, as (remote) merchants know that few customers will be complaining, because of the high costs involved. In the most extreme case, a merchant might be hard, even impossible to identify; Such a merchant only has an IP address that can be used to take contact with a server residing somewhere on earth.

In order to deal with such problems and in order to support Europe's transition to a knowledge-based economy and boosting competitiveness, the European Union (EU) has published a number of directives to deal with this kind of problems. Thus, in this case, the EU electronic commerce EU directive that has recently been approved [3], defines clearly that merchants should have a place of establishment and show all their identification and contact information on the site. As place of establishment is defined the place where the merchant actually pursues an economic activity through a fixed establishment, irrespective of where the web-sites or servers are situated or where the merchant may have a mail box. This removes legal uncertainty and ensures that merchants cannot evade supervision, as they will be subject to supervision in the country where they are established.

Also, the establishment of ICANN¹ in October 1998 is indirectly and partly contributing in alleviating this problem, i.e. in identifying merchants. It is expected that by October 2000, ICANN will have taken the responsibility for coordinating the management of the Domain Name System, the allocation of Internet Protocol address spaces, the coordination of new Internet protocol parameters and the management of the Internet's root name server system [19].

¹ Internet Corporation for Assigned Names and Numbers

Regarding what law to apply in contracts² and disputes³, the E-Commerce Directive does not deal with the application of the Brussels Convention [16] on jurisdiction, recognition and enforcement of judgements in civil and commercial matters. Furthermore, the Directive doesn't interfere with the Rome Convention [17] as regards the law applicable to contractual obligations in consumer contracts or with the freedom of the parties to choose the law applicable to their contract. Also, this Directive doesn't affect the law applicable to contractual obligations relating to consumer contracts. It has to be mentioned that the location of the customer at the time of putting the order doesn't make any difference, as it is the customer's permanent location that counts. Therefore, the law of the country s/he has his habitual residence is the one that governs contractual obligations.

Out-of-court dispute settlements are encouraged in the EU Directive [3]. This type of mechanism may appear particularly useful for some disputes on the Internet because of its low transactional cost, which is bearable for small businesses and individual customers, who might otherwise be deterred from using legal procedures because of their cost. Thus, individual EU countries have to ensure that in the event of disagreement between a provider and its recipient, their legislation allows the effective use of out-of-court schemes for dispute settlement, including appropriate electronic means. The EU directive suggests that the legal framework of these dispute-settlement mechanisms in the various countries should not be such that it limits the use of these mechanisms or makes them unduly complicated. Thus, in the case of specific mechanisms for disputes on the Internet, these could take place electronically.

C. Pricing, Payments, Intellectual Property Rights And Taxation

Pricing of digital goods (provided that the copyrights are owned by the producer/distributor) and services is affected by the fact that perfect copies, or replicates, can be reproduced and distributed almost without any cost [10]. Furthermore, new opportunities for repackaging content through bundling, site licensing, subscriptions, rentals, differential pricing, per use fees and various other mechanisms have emerged with the use of Internet [1].

Other questions are related with the tracking and recording revenues and especially, of literal and artistic works: who

² Consumer organizations demand the application of the consumers' home country legislation. Merchants are demanding the freedom of choosing from consumer or merchant home country legislation. One suggested solution would be that in the case of certified sites (certification of consumer protection methods) the law of the merchants' home country could be chosen as the applicable law. In the case on non-certified sites the law of the consumer's home country would apply.

³ The Commission has suggested that consumer always has the right to rise an action against the merchant in the court of the consumer's residence. The businesses are strongly against this solution arguing that it would increase speculative transnational b-to-c electronic commerce.

collects the payments, how the revenue is calculated and who is responsible for copyright protection and transfer of funds. The issue is resolved in EU's directive proposal [4], which follows the globally accepted Berne convention, its amendments, and WIPO⁴-recommendations. Most often Intellectual Property Rights (IPR)-owners transfer their rights to representatives, who grant the permit to use the material on request, generally by pricing the rights according to the quality and extent of use (e.g., public/private - no of copies to be sold). The producer or 'packager' is then responsible of paying on the use of works, protecting against copyright infringement, illicit tampering, etc. The telecom operator, however, is not responsible, unless the material is clearly illegal, harmful, for details see [5]. In digital economy this means that customers pay on a packaged product to the producer, and on browsing, when having a look upon the material on a web-site. In the former case the IPR-owner can definitely gain while in the second case, the profit depends on the agreement with the seller and whether or not the customer is allowed to browse free of charge. It seems that in some cases the operator is willing to provide copyright protection mechanisms, packaging, delivery, and charging for the packaged product as value-added services to the representatives of the copyright owners (e.g. [5]).

Regarding charges such as customs, the joint EU-USA declaration on e-commerce (see [22] and the EU directive [3] states that when goods are ordered electronically and delivered physically, there will be no additional import duties applied. In all other cases relating to e-commerce, the absence of duties on imports should remain.

Concerning Value Added Taxation (VAT) the situation is changing. The problems associated with VAT together with proposed remedies can be found in [20]. The main goal is to collect VAT for Information Society Services (ISS) that also cover trading of electronic goods provided that they are consumed within the EU, no matter where the order is placed and how the goods are delivered to the customer. The Directive proposal requires larger service providers based outside the EU to register themselves in one member country and to collect and remit VAT for the EU resident private consumers purchasing physical or digital goods using EC facilities. On the other hand, the proposal allows EU based service providers to sell goods without collecting VAT, provided that the goods are consumed outside the EU. This rectifies the double unfair situation for EU merchants where merchants outside the EU have been able to sell goods for customers within the EU without collecting VAT, while EU resident merchants have been obliged to collect VAT for goods electronically ordered and exported also for consumption outside EU. Notice that the rules for businesses will not be changed, i.e. the reverse mechanism is further applied as before in collecting VAT.

Another matter with taxation, has to do with who is liable for paying VAT, the customer or the merchant? The latest

⁴ World Intellectual Property Rights Organization

directive proposal on taxation matters [20] tries to clarify the place of taxation as follows:

- for services supplied by a non-EU merchant to an EU customer the place of taxation will be within EU and therefore subject to VAT, while in the opposite case, i.e. for services supplied by an EU merchant to a non-EU customer, the place of taxation will be where the customer is located and therefore they will be not subject to VAT within EU.
- for services supplied by an EU-merchant to another business in another EU country, the place of supply will be the place where the customer is established while for services supplied by the same merchant to a private individual in the EU or to another business in the same EU country, the place of taxation will be where the supplier is located.

Although intuitively appealing, the rules described raise some questions. Possible criteria for determining the place of consumption, definitions for place of supply, taxable person and related issues can be found in [21]. The place of consumption in [20] is determined through the domicile of the private consumer. That is, if a person has a permanent address in Finland, it is within EU, no matter where the person actually resides and consumes the product. This works rather well for purchases made by fixed equipment, like home PC, but for mobile terminals there are problems involved. The product, e.g. digital map, can be consumed in USA, although purchased and downloaded from a merchant in Europe. On the other hand, a person with domicile in USA can come to Europe and order local digital map to mobile terminal, evidently not paying the VAT, because her domicile is in USA. How can a merchant determine when to collect VAT, when not? Evidently, the only way is to ask the customer to give information on the domicile. The identity of the mobile terminal (phone number or IP number) is not enough because it can be misleading. In the future, when there will be more mobile devices at the disposal of the customers and more products like digital maps usable in them, this principle can lead to a considerable VAT avoidance by non-EU citizens who come to the territory of EU for longer periods of time, but have their domicile outside EU.

A further issue that arises is how it can be checked if the VAT has been paid properly. If both merchant and customer are businesses in the EU this is easy to be checked, as they are both registered for tax purposes. But in case of individuals or in case of merchants from non-EU countries things are not so simple. In order to deal with such issues, in the same proposal [20] it is suggested that non-EU merchants don't have to register for tax purposes if they supply products to business EU customers, as the latter are responsible for the VAT. Regarding supplies to individuals, they have to register only if their annual level of sales within the EU is below 100.000 Euro, in order to avoid placing undue burdens on the development of international e-commerce and in particular on very small businesses or on those who only occasionally make sales to

EU customers. But, overall, this measure puts EU and non-EU merchants on an equal basis when they supply to EU customers.

III. CURRENT MOBILE TECHNOLOGIES

A. General Definitions

The term mobility refers to the ability of a user to change location. We view the issue of mobility from the point of view of a customer changing physical location (city, country, continent) together with his/her mobile hand-held terminal, as this will possibly cause complications for conducting trade. Note, that this differs from 'normal' Internet connection, that is - so far - assumed to take place between particular physical location (that is, the IP addresses involved can be mapped to a fixed physical location on earth). In general, merchants can also be mobile, but this does not actually make any difference, because, according to the proposed legislation they must have a physical 'place of establishment' and this is what matters in legal sense. Technically, however, a mobile merchant poses new challenges.

We view the current situation according to the following picture. The backbone network is an IP network (Internet) and the servers are attached to it. Mobile hand-held terminals as facilitated by Mobile IP technologies connect directly within the IP network [11] or by access technologies, like 2G GSM networks or 3G networks⁵. One of the main differences between these different network generations is the bandwidth. In the current 2G networks the bandwidth ranges from 9.6 kbps to 14.4 kbps. In 2G+ HSCSD (High Speed Circuit Switched Data) will offer in practice 57.6 kbps and GPRS (General Packet Radio Service) ca. 112 kbps transmission rates. The EDGE (Enhanced Data rates for Global Evolution) promises 384 kbps maximum, but in practice the transfer rates are below that. 3G networks should provide 2 Mbps in good circumstances. In worse circumstances (e.g., weak signal, or in the move) the bandwidth will be only a few hundred kbps.

Another dimension of the access networks is the service capability. In the basic 2G network the services are voice, circuit switched data (CSD), and short messages (SMS). Especially short messages have been used to support financial services like banking and stock services. CSD can be used as the carrier in a TCP/IP network and it is possible now to do Internet banking using e.g., hand-held Communicators over CSD. Note that in some European countries e.g. balance inquiries can be made also over a voice interface by any GSM phone and the balance report can be either listened or received as a short message into the handset.

⁵ 2G = 2nd and 3G = 3rd generation mobile networks. 2G+ is an acronym for amended 2G networks e.g. WAP.

In 2G+ networks the new standard Wireless Application Protocol (WAP) [14] provides a novel way to support MEC. It brings Internet and GSM technologies together so that contents in WWW servers can be automatically reformatted and moved to handsets. E.g. basic banking services are already made possible through WAP phones [9]. It is expected that the WAP technology will be adopted in the 3G systems, too. The major technical difference to 2G+ systems is the considerably better bandwidth, close to the present LAN-connections. In Japan, technology called I-mode has been lately introduced that serves similar purpose as WAP [23].

Bluetooth [2] is a new emerging technology that will evidently have impact on MEC. Using this technology it would be possible to conduct e-commerce transactions without a heavy network infrastructure. Thus, handheld devices could talk directly e.g. with cash registers. Currently integration of Bluetooth and WAP are under way [14].

B. Mobility In B-To-C E-Commerce And Its Ramifications

The mobile hand-held terminals together with WAP are a new access technology to Internet-based E-commerce world. As such, E-commerce based on WAP services does not change the structures at the Internet side. So the business processes might remain the same as when the access to them is performed using PCs. There are still some legal and technical issues that will make a difference. Technically, mobile hand-held terminals are much smaller in size than PC's and bandwidth is still scarce. This makes the conduct of the whole transaction from Information Acquisition to Execution phases expensive, especially if there is lot of data to transmit. For example, the proposed legislation requires that a lot of information about the ISS provider and contract is transmitted, before the deal can be closed. Additionally, AV marketing information consumes a lot bandwidth. Thus, there is a need to adapt the E-commerce services into the WAP world, and mobile world in general.

Considering security and identification of the terminals, the latter is at about the same level as in stationary PCs over a public telephone network. Actually, the phone number on the SIM card is more persistent than the IP-identity of PCs that can be easily changed. On the other hand, authentication of a person should not be based on SIM card identity or the device identity, because both can be stolen. Although the access is protected by PIN, these are at least currently rather short (4 digits) and besides this, if the terminal is stolen while it is on, the PIN is not at all asked. In practice, this would call for improved identification and security.

From the legal point of view, customers' mobility poses new challenges. The question is according to which legislation the business is conducted. The natural candidates

are the legislation of the residence country of the service provider, legislation of the residence country of the customer, and legislation of the country of the customer's residence. USA seems to favor the first alternative (the merchant sites announce that the applicable law is that of their residence). In EU the current legislation is based on Rome and Brussels Conventions [17, 16] and the new Directive on E-Commerce [3] (see above).

However, since the geographical location of a mobile user with a hand-held terminal can be easily identified⁶, there emerge a lot of services in MEC that can utilize the location information (or that of the terminal, to be exact). The evident ones are answers to questions like "Where am I now?", "Where is the nearest X?", or "Where is Y now". Another group of location-related questions are of type "Where is the cheapest X nearest to Y/me?". To facilitate these services, new solutions are required. One question is, how the location information is provided in the case of the questions of the first type. Maps are an answer, but there might be others, too, like global coordinates. The latter are basis for the location services in any case. If maps are used, the interesting question is, how are the costs and the economic yield of the service divided among the players. Clearly, the digitized maps and other location-based services are digital goods and thus regulated by [15].

Technically it would be possible in the near future to track the location of the terminal precisely enough in order to determine the place of consumption of electronic goods. This would alleviate some of the problems discussed above with respect to taxation. To really use this kind of mechanism would require changes in regulations and also a lot of technology development.

IV. TRANSACTIONAL REQUIREMENTS FOR MOBILE E-COMMERCE

A. Issues And Definitions

Traditional transactions are used to encapsulate database operations so as to provide Atomicity, Consistency, Isolation, and Durability (ACID). They provide clean semantics to concurrent executions and a powerful abstraction for an application developer. Since the beginning of 1980's new transaction models have been developed to support new application areas, like computer supported cooperative work, workflows, computer integrated manufacturing, international banking, etc. There is a rather comprehensive overview on the earlier work in [6] and some later developments are discussed e.g. in [24] and [25].

⁶ User's location can be identified in a variety of ways: the terminal can be triangulated based on the location of the terrestrial stations, whenever the phone is on. The phone itself can embed GPS. The phone can also be identified at an external network node, e.g. when paying by phone at Bluetooth terminal (e.g., cash register, the location of which is known.)

What differentiates MEC from the earlier environments studied, from transactional point of view is a number of issues which are analyzed in the following. The first issue is the possible hostility of the open environment. From transactional point of view that means that there is a risk that the parties engaged in an E-commerce transaction might be more easily disguised or forged ones. For instance, the merchants server might not be the one the client thinks it is, or during the E-commerce transaction another entity "hijacks" the transaction and disguises as the client changing e.g. the ordering address of the delivery or changing the amount paid. These kind of malicious transactional components need not be considered in a traditional environment.

Another issue that is related with the previous one is the vulnerability of the mobile hand-held devices. They can easily be stolen and misused. Thus, from transactional point of view, the transactional mechanism should not rely on the device identity (such as phone number or IP number) and it should not deduce user's identity based on the device identity. Thus, even if an E-commerce transaction was started by the user really possessing the device, the device might have been stolen in the meantime and the fraudulent person might change some parameters of the ongoing E-commerce transaction later in his/her benefit. The main issue is, however, that new E-commerce transactions might be started by the stolen device such that the real owner would be charged for them.

There are, on the other hand, great opportunities for useful applications that are based on the device = user identity assumption or anonymous payments based on E-cash carried within the device; consider e.g. using a bus in any city just walking into it with a hand-held device in the pocket and accepting the payment by one touch of a button. Or paying gasoline at a gasoline station using a hand-held device (e.g. a WAP phone). Therefore, the transactional mechanisms should not be either or but rather both and. The user could specify the security level he or she wants in a particular case.

Third issue that is closely related with the mobility concept is the communication autonomy (C-autonomy, see e.g. [12, 13]) of the devices. It means that the devices are not always reachable through the network and that it is natural that they are rather often disconnected. This can happen for many reasons, for instance because simply the user shuts off the connection, the device runs out of battery, or because the device is outside the coverage area.

From transactional point of view this means that transactional mechanisms should not assume continuous capability of the terminals to communicate, nor should expect that there would be periods during which the terminal is able and willing to communicate with other components with (nearly) 100 per cent certainty. The previous considerations suggest that transactional mechanisms must be tied with closer with security

mechanisms. How should this be done? This is discussed in the following subsection where a real world example is examined.

B. A Real World Example Of An E-Commerce Transaction Applying Internet Banking

Keltainen pörssi is a company in Finland [19] that acts as a mediator between private people wanting to sell or buy something, i.e. it maintains an electronic market place. In the past, they only published a newsletter but a couple of years ago the company has expanded the newsletter into an electronic one on the web with an extensive search engine on top. The customer can place offers for free, but searching for them costs.

In the following we examine the process of ordering a service and paying for the service charge to Keltainen Pörssi, i.e. it is a question of b-to-c transaction (see [19] for details). The service charge can be paid in several ways, one of them being a direct bank transfer at a bank. Figure 1 depicts the structure of this transaction.

There are three parties, the customer, the service provider (merchant), and the bank. The merchant and bank must have standardized the information content and format sent between them (via customer and directly); otherwise an application could not process it. The merchant can be very sure that it got the money from the customer wanting the service if the bank acknowledges the transaction. This is because the funds are moved immediately from the customer account to the merchant account when the customer acknowledges the sum.

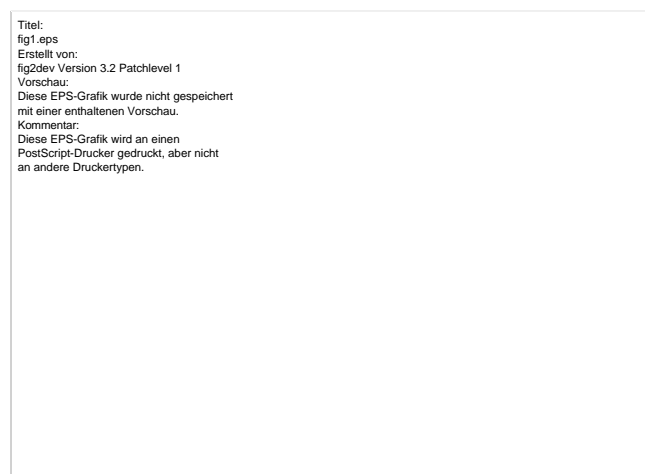


Figure 1. Keltainen pörssi: the overall scheme (<http> or <https> interactions)

From transactional point of view the system is rather vulnerable, because if the customer would not exit the service of the bank with "end button" it would be highly probable that the merchant would not consider the payment to have succeeded and would deny the mediator service, although it was paid. The same holds if it does not get the

confirmation from the bank about the payment although it got the end-button confirmation from the customer. The latter situation occurs when the customer either did not go at all to the bank and tries to cheat the merchant or when the customer contacted the bank that made the funds transfer but failed before it was able to confirm the payment to the merchant. The merchant would probably assume the first case and would deny the service - until the status of the payment has maybe been manually checked.

In general, the activities between merchant, customer and the bank should be seen as one distributed transaction that should be run in an atomic way. The atomicity condition covering the situation could read: the service must be granted by the merchant if and only if the customer pays the service.

Looking at what happens at the parties, one understands that at each party there is a (business) process instance running. The arrows (i.e. messages) coordinate the advancement of the processes. The explanatory text can be understood as steps of the processes. In order to achieve the atomicity above, all processes must run into end that is coherent with those of the other processes. This is the distributed atomicity requirement. Notice, that at the customer site the process is manual, whereas at the merchant (service provider) and at the bank it is fully automatic through one or more applications. Thus, the customer process cannot store its state into the computer/terminal. The other two processes store the state of the process in a durable way; When Keltainen Pörssi asks the customer to pay for the service, it stores the status of the process into a database and commits it (something like customer #, X euro, TID, TIME). Correspondingly, when the customer has transferred the funds, it is recorded at the bank in a permanent way using a database transaction. Further, it is taken care of that the confirmation is delivered in an indivisible operation to the merchant. Thus, durability in this context guarantees that the process states, including the sent messages, are recorded in a crash-resilient way.

If we look at consistency, in this context we can differentiate between three separate issues. First, each individual step at the players must preserve database consistency in a traditional sense. For instance, the customer cannot transfer funds if the credit limit on his/her account would be exceeded as a result of the transfer; the address and phone number given by the customer should be (syntactically) valid ones. Second, each involved process should end in an acceptable end state, i.e. run into end. For instance, the process at the bank should move the funds and announce the success to all other parties or should not move the funds and announce it at least to the customer. Stopping before the announcements would mean that it did not run until end. Correspondingly, the process at the merchant should end either with granting the service or denying it and announcing the decision to the customer. Third, all the processes should end in a globally coherent state that satisfies the distributed atomicity requirement.

The steps of the processes should be isolated from the other steps in such a way that there are no concurrency anomalies. This can be often guaranteed by isolating the single steps like the funds transfer, but there might be cases in which larger portions, i.e. several steps of the processes should be run in an isolated mode.

The above case fulfills the requirement that the transactional mechanism is tied with security. All communication with the bank happens in an encrypted form (using https) and the same is possible with service provider. The funds transfer also requires human being that reads the two required PINs from a piece of paper. Thus, the service cannot be ordered by computer alone. A fraudulent person misusing the service should have the PIN slip of the customer of the bank, and in addition the six-digit long userid of the customer at the bank. The latter cannot be deduced from the PIN slip or account number.

Reflecting this into mobile world, where the customer would use a hand-held device when issuing the transaction, the same conclusions would hold. There is still one problem with such a piece of paper -approach to the authentication: it is rather awkward to drag such paper slips around while on travel. The user might also tend to write down the six-digit long userid. Thus, if the PINs of the bank service are stolen along the userid while travelling, much damage might result. Therefore, more clever mechanisms should be invented, like storing the PINs or similar things on the terminal (or the SIM card) or using some other authentication mechanism more suitable for the network environment.

Current commercial solutions include: 1) Smart trust type solution card by Sonera [18], where the PKI private key is on the SIM card and is used for authentication and non-repudiation, 2) the solution offered by Nokia, Merita and Visa, where security mechanisms are incorporated into the software and hardware of the terminal in such a way that the terminal has a credit card capability and 3) the solution offered by Motorola and MasterCard that offer hand-held terminals equipped with a credit card reader.

All these solutions have, however, weak points. In smart trust solution the usage of the private key is protected by 4-digit PIN. Thus, the real level of security, authentication and non-repudiation depends on how carefully the PINs are kept secret by the customers. The length of the private key (1024 bits) does not decide in this case. Case 2 is similar in the sense that the access to the device is protected by some identification mechanism. The length of the PIN and the number of PINs required to perform a MEC transaction might be larger than in the previous case. The problem with longer PINs or passwords is, however, that users are not able to memorize them and are forced to store them in some form. This makes them again vulnerable to theft. In case 3) the thief should in the safest case steal both the device and the credit card and know or guess the PIN of the device and/or the credit card in order to be able to

initiate forged transactions. The highest security has the case where a particular credit card could only be used with a particular device and both have own PINs. If a particular credit card could be used with any device, then this case is identical with stealing the credit card and guessing the PIN. Business could also be performed by fabricated credit card copies in this case.

Another - and orthogonal thing to the previous ones - is that while ordering the service through a C-autonomous and error-prone mobile hand-held device, it is to some extent likely that the process at the customer side stops and the status information is lost (cf. running out of battery or coverage while paying). For these kind of situations the terminal should have failure resiliency and capacity to recover the process into a consistent state. In practice, this would require that the data obtained from the merchant that contains the transaction identifier and the details of the payment etc. should be stored persistently along the process state indication "transfer in progress". The application at the bank should also accept a new connection attempt after the crash with the same transaction id. These are typical transactional requirements for the implementation of the service.

The above example is simple in the sense that when the funds have been transferred and this is known by the merchant (in this case a service provider), the service can be opened and all parties are satisfied. If it is question, however, of providing tangible goods, like books to the customer, the situation becomes more complicated. First, the process at the merchant runs days or weeks instead of a few minutes. Second, the customer can return the book and thus cancel the purchase in 30 days (21 days, this varies according to the legislation). Third, the purchased item can be rather valuable, like a car. For these reasons the customer could get more check points to the process running at the merchant. The current practical situation is that the customer confirms the order and after that the merchant does not require any acknowledgments from the client, although it might send some information to the client about the state of the process instance using email.

The EU directive [3] adds nothing to the de-facto situation i.e. it requires that the merchant confirms the order by electronic means (article 11 of [3]). Tracking other phases of the process are not addressed. Especially after-sale phase is outside the explicit scope of the directive.

On the other hand, the process at the merchant and customer could be described in a more detailed way in the national legislation, but whether this makes sense from flexibility point of view is questionable. Different mechanisms in different countries might hamper the trade. This should be studied further.

Transactional mechanisms can be used in letting the customer to control at several points the merchant process, like separately confirm the delivery of the goods ordered and separately confirm their arrival. This would make it less

probable that somebody misused e.g. the credit card and ordered goods with it. The intermediate checks alone do not help very much, because a fraudulent person might manage to perform all the checks (based on email, for instance). If, however, each check would require a personal identification, like a private key, this would become rather difficult. Again, thinking about the mobile hand-held terminals, could the private key be stored into them safely so that a fraudulent person stealing the device could not take benefit of it? The idea that the SIM card contains keys like in Smartrust [17] does not help much in security sense, because the keys are stolen with the device. The actual level of protection is that of the (4-digit) PIN.

One solution is to have a separate device that contains the private keys and that can communicate with the hand-held terminal. Another idea is to keep the PIN partially on a server. This had been investigated closer in [26].

For a more detailed treatment of the transactional aspects the reader is urged to consult [27]. The practical work is continuing within the framework of Multimeetmobile project, where we will implement a transactional mechanism (see [28]).

V. CONCLUSIONS

Business to Consumer E-Commerce of almost every type of good or service is thriving the last few years. At the same time, there is a remarkable increase in the number of internet-capable mobile hand-held devices (cf. WAP phones) that is expected to overtake very soon the number of PCs and other workstations, therefore the investigation of the effect of this situation on E-Commerce seems important. In this paper we investigated issues related with the b-to-c E-Commerce in an environment where a mobile customer initiates and concludes e-commerce transactions using his/her mobile hand-held terminal. This type of e-commerce is interesting from many points of view. The small displays and the scarce and expensive limited bandwidth may discourage the user to visit many sites and negotiate with different merchants; however, the use of mobile hand-held terminals opens a new business area in E-Commerce, the location based services, and new e-commerce scenarios seem to emerge.

We consider mobile hand-held terminals as access technology to Internet. As such, some of their characteristics like their embedded payment facilities, the secure identification mechanism guaranteed by the operator (phone numbers) and protected by PIN, facilitate respective issues in E-commerce transactions. However, others characteristics, like their limited graphics capabilities, limited bandwidth, C-autonomy and their vulnerability result in a number of interesting implications from legislative, security, application and transactional point of view.

Furthermore, when a transaction is initiated by a mobile hand-held terminal, its part that is related with the execution of the business processes at the various sites, i.e. at the merchant's site or at the bank's site, remains the same. What is affected by the customer's mobility is the part of the transaction related with customer identification, as mobile hand-held terminals can be easily stolen and appropriate end-to-end mechanisms are needed to guarantee customer identification.

Therefore, the pervasive orthogonal aspect in MEC is security and privacy as well as distribution aspects that deal with the global coherence of processes. Business processes might be different in different regulatory frameworks (EU, USA, Japan) and this may have certain impact on the transactional mechanism in a mobile hand-held device that should recognize the process type at the merchant's site.

These are some of the issues need further investigation. The work presented here depicts the results of our on going research in the area of mobile computing and electronic commerce.

ACKNOWLEDGEMENT

The authors would like to thank Prof. Jukka Heikkilä from the University of Jyväskylä and Mr. Juha Laine from Helsinki School of Economics for their comments and contribution in earlier drafts of this paper.

REFERENCES

- [1] Bakos, Y., Brynjolfsson, E. (1997). Aggregation and Disaggregation of Information Goods: Implications for Bundling, Site Licensing and Micropayment Systems, Working paper, MIT, June, 1997. <http://www.gsm.uci.edu/~bakos>
- [2] www.bluetooth.com, data accessed June 30, 2000.
- [3] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce"). Official Journal of the European Communities, Vol. 43, L178 (17.7.2000). Also available at http://europa.eu.int/eur/lex/en/oj/2000/l_17820000717en.html.
- [4] Proposal for a European Parliament and Council Directive on the harmonization of certain aspects of copyright and related rights in the Information Society (final). http://158.169.50.70/eur-lex/en/com/reg/en_register_1720.html
- [5] Amended proposal - Proposal for a Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks (Commission Proposal - COM(98)784 final). http://158.169.50.70/eur-lex/en/com/reg/en_register_132060.html
- [6] Ahmed Elmagarmid (ed.): Database Transaction Models for Advanced Database Applications. Morgan-Kaufmann Publishers, San Mateo, USA 1992.
- [7] Guttman, R.H., Moukas, A.G., Maes, P. (1998). Agent-mediated Electronic Commerce: A Survey, Software Agents Group, MIT Media Laboratory, Knowledge Engineering Review, June 1998.
- [8] Kambil, A., van Heck E., (1998). Re-engineering the Dutch Flower Auctions: A Framework for Analyzing Exchange Organizations, Information Systems Research, Vol. 9, No. 1 (March 1998), pp. 1-19.
- [9] www.merita.fi, data accessed June 30, 2000.
- [10] Shapiro, C., Varian, H.R., (1999). Information Rules: A strategic guide to network economy, Harvard Business School Press, MA., USA, 352 pages.
- [11] Tanenbaum, A.S., Computer Networks (3rd edition). Prentice Hall, Inc. USA 1996.
- [12] Jari Veijalainen, Frank Eliassen, Bernhard Holtkamp: The S-transaction Model. Chapter 12 in [6].
- [13] Jari Veijalainen, Transaction Concepts in Autonomous Database Environments. (Ph.D. thesis). GMD-Bericht Nr. 183, ISBN 3-486-21596-5. R. Oldenbourg Verlag, Munich, Germany, April 1990
- [14] <http://www.wapforum.com/>
- [15] Brussels Convention on Jurisdiction and the enforcement of judgements in civil and commercial matters (consolidated version); Official Journal C027 of 26/01/98 (498Y0126(01)). Available at <http://www.ispo.ccc.be/ecommerce/legal/favorite.htm>
- [16] Rome Convention on the law applicable to contractual obligations (consolidated version) Official Journal C027 of 26/01/98 (498Y0126(03)). Available at <http://www.ispo.ccc.be/ecommerce/legal/favorite.htm>
- [17] www.sonera.fi, data accessed 29 June 2000
- [18] www.keltainenporssi.fi, data accessed June 30, 2000 (in Finnish).
- [19] Communication from the Commission to the Council and the European Parliament. The Organisation and Management of the Internet - International and European Policy Issues 1998 - 2000. COM(2000) 202 final. Brussels, 11.4.2000
- [20] Proposal for a Regulation of the European Parliament and of the Council on administrative cooperation in the field of indirect taxation (VAT) and Proposal for a Council Directive for VAT arrangements applicable to certain services supplied by electronic means. COM(2000) 349 final. Brussels, 7.6.2000
- [21] Working Paper of the Commission on Harmonisation of turnover taxes. XX/98/0359, 3.4.1998
- [22] See www.amazon.com
- [23] www1.freeweb.ne.jp/~cross/i/index.htm
- [24] DeBy, R. Klas, W., Veijalainen, J. (eds.). Transaction Support for Cooperative Applications. Kluwer, 1997
- [25] Elmagarmid, A., Rusinkiewics, M. Sheth, A. (eds.) Heterogeneous and Autonomous Database Management Systems. Morgan-Kaufmann 1998.
- [26] Tang, J., Veijalainen, J. Using Agents to Improve Security and to Assist in Negotiations for E-Commerce Transactions. Paper accepted to HICSS-34, Minitrack on Mobile E-Commerce. Hawaii, USA, January 3-6, 2001.
- [27] Veijalainen, J. Transactions in Mobile Electronic Commerce. In: Gunter Saake, Kerstin Schwarz, Can Turker (eds.). Transactions and Database Dynamics. Lecture Notes in Computer Science, Nr. 1773, Springer Verlag, Berlin, December 1999, pp. 208-229.
- [28] Multimeetmobile site at www.cs.jyu.fi/~mmm

ⁱ The research was supported by the Finnish National Technology Agency under contract 330/401/99.

ⁱⁱ The research was supported by the Finnish National Technology Agency under contract 750/401/99 and has been performed while Aphrodite Tsalgatidou was on a leave of absence from Department of Informatics of the University of Athens, Greece. E-mail: afrodite@di.uoa.gr