Proceedings of
National Conference on Innovative Trends in Computer Science Engineering (ITCSE-2015)
held at BRCMCET, Bahal on 4th April 2015

# Security Issues and Trends of M-Commerce in India

Snehlata
Lecturer, Govt. College for Women, Bhodia Khera, Fatehabad (Haryana)
ms.snehlata15@gmail.com

**Abstract:** The purpose of this research paper is to identify factors affecting the adoption of M-commerce. The
Significant growth of M-commerce application is remarkable in India. More and more consumer is transferring to M-commerce to achieve better and fast transaction into market. M-commerce is complex in nature and includes changing procedure in market. M-commerce is emerging level in India. The astounding rate growth in mobile penetration in India, higher mobile technology and networking is coming day by day. Now a mobile phone is not only use for text SMS or phone call but also be used for many other activities like browsing of internet chatting or other virtual activities .This research paper identifies the factors affecting the adoption of M-commerce. This paper theoretical contribution is to explain the how M-commerce is developing in India and to identify clear contexts and assistant mechanism.

**Keywords:** Wireless technologies, M-commerce, Security and Bluetooth.

## I.INTRODUCTION

Mobile is becoming the dominant means for accessing communications primarily because deploying mobile network is not only more cost-efficient but also mobile provides greater flexibility and convenience to its subscribers

the m-commerce market [1, 4, 8] . Firstly, m-commerce holds a promising future due to the penetration of the mobile phone market. Widespread availability of devices can be utilized by suppliers to directly communicate to existing and potential customers. Further, the push from vendors, attractive content, low costs and reasonable prices of the mobile services, substitution possibilities are also promoting substantially the market growth. Secondly, some technology-related factors, such as improvement of bandwidth, development of wireless Internet and software, emergence of new technologies and so on, contribute a great deal to the development of m-commerce market. In addition, some social tendencies, including so-called handset culture and increasing propensity to transact online, can be regarded as another driving force for prosperity of m-commerce. All of these market drivers enable m-commerce to be an inevitable trend on which businesses should focus their attention. Therefore, it is important for the numerous participants to understand the unique features, framework and possible issues of m-commerce so as to grasp the new business chance and enhance their competitiveness in the future m-commerce market.

## II.LITERATURE REVIEW

The study by Kisieloweska-Lipman (2009), 'Pocket Shopping: International consumer experience of buying goods and services on their mobile phones', coordinated by the UK consumer group Consumer Focus, provides useful data on the consumer experience of purchasing goods and than landline telephone (Sanjay, 2007). At present, there are a variety of definitions for m-commerce used in different kinds of sources and literatures [1, 7, 10, 11].

From computerworld.com, "Mobile commerce is the use of radio-based wireless devices such as cell phones and personal digital assistants to conduct B2B or B2C transactions over wired, web-based e commerce systems." The definition given by Searchingmobilecomputing.com shows that "M-commerce (mobile commerce) is the buying and selling of goods and services through wireless handheld devices such as cellular telephones and PDAs." Furthermore, according to the definition given by Tarasewich, P., Nickerson, R.C. and Warkentin, M. in their paper "Issues in mobile commerce"[10], "Mobile e-commerce (mobile commerce or m-commerce) is defined as all activities related to a commercial transaction conducted through communications networks that interface with wireless (or mobile) devices. These definitions provide us with an overall image of m-commerce, which describes m-commerce as a commercial activity involved in electronic financial transactions by using wireless devices. There are different driving factors that encourage businesses to make advance towards services via mobile devices. Consumer groups from across the European Union, Asia and North America participated in the study. The study made a number of findings including that:

- The availability of information during a m-commerce transaction can be limited by technological constraints such as a phone's small screen size
- The m-commerce market is still developing and is in the early stages when it comes to the range of products and services available to consumers
- The most common products purchased include mobile premium rate services (PRS), e-tickets, digital content (other than mobile PRS) and physical goods
- Purchasers faced difficulties seeking redress or accessing dispute resolution mechanismsm-commerce transactions are susceptible to fraud and unauthorised payments.

1999 Guidelines were adopted to provide guidance to government, industry and regulators when developing protection mechanisms for consumers engaging in online shopping. The OECD's 2008 Policy Guidance for Addressing Emerging Consumer Protection and Empowerment Issues in Mobile Commerce examined the applicability of the 1999 Guidelines to m-commerce. In general, the 2008 paper found that the 1999 Guidelines were adequate but it noted that policy makers should consider challenges within the market in relation to information disclosure, dispute resolution mechanisms and the security of transactions. Given developments in technology since 1999, and the findings raised in 2008 at the Ministerial Meeting on

the Future of the Internet Economy (at Seoul), a review of the 1999 Guidelines commenced in 2009.

Communications expert Paul Budde's paper, 'Australia - Mobile Data - Mobile commerce and M-Payment' (2010), provides an overview of the m-commerce marketplace in Australia and identifies factors that will be important for the growth of the market in coming years. Budde contends that the m-commerce marketplace in Australia is relatively small in comparison to Asian markets, especially Japan and South Korea.

## IV.PURPOSE OF THE STUDY

Mobile commerce has become the latest topic for today. Business organizations have been restlessly evaluating the revenue potential of the m-commerce market and developing business models to exploit the huge profit potential of this new market. So the main purpose of this paper is to:

- Provide an brief description about mobile wireless technologies.
- Understand unique feature and benefits of m-commerce.
- To analyze various factor that affecting m-commerce.
- To analyze trends of M-commerce of India.

**Research Approach**

In an attempt to learn as much as possible about the Mobile Commerce, we conducted in depth research to obtain most of the necessary data. Through content analysis of firm disclosure data, historical data analysis, company case studies, and sector reports, we gained much valuable information pertaining to our research. We used secondary sources of data collection such as the Internet, websites, books and magazines etc.

## III. UNIQUE FEATURES OF M-COMMERCE APPLICATIONS AND SERVICES

MEC applications take advantage of mobile communications to offer to consumers and businesses additional benefits as opposed to traditional e-commerce applications are:

Location-awareness: In mobile computing, knowledge of the physical location of a user at any particular moment is central to offering relevant services. The location of a mobile device is available to the mobile network operator but it can also be found using sensor devices or technologies such as the Global Positioning System (GPS). GPS uses a number of satellite stations to calculate with great accuracy the location of devices equipped with GPS receivers. There are many examples of location based electronic commerce applications including: geographically targeted advertising (everyone near a fast-food restaurant gets free (electronic) coupons for the new burger), fleet management, vehicle tracking for security, traffic control, telemetry, emergency services, etc.

Adaptively: Mobile e-commerce applications should be adapted to the environment of their clients. Adaptability is possible along various dimensions including the type of the device in use, the currently available communication bandwidth as well as location and time.

Ubiquity: Mobile communications enhance electronic commerce by making electronic commerce services and applications available anywhere and at anytime. Through hand-held devices such as mobile phones, users can be reached at anytime, independent of their location. Mobile computing makes possible that users are immediately notified about particular events. It also enables the delivery of time-sensitive information whose value depends on its timely use.

Personalization: The information, services and applications available in the Internet today are enormous. It is thus important that the user receives information that is of relevance. Furthermore, customization is a key issue in using mobile devices because of the limitations of the user interface in terms of size, resolution and surf ability. Studies (Durlacher Research, 2000) show that every additional click reduces the transaction probability by 50%. Thus, MEC applications must be personalized enough to represent information in compact and attractive forms and to optimize the interaction path, enabling the user to reach the desired services with as few clicks as possible.

Broadcasting: Some wireless infrastructures, such as cellular architectures and satellite networks, support broadcasting (i.e., the simultaneous delivery) of data to all mobile users inside a specific geographical region. Broadcasting offers an efficient means to disseminate information to a large consumer population. This mode of operation can be used to deliver information of common interest to many users such as stock prices, weather information or for advertising.

**The benefits of Mobile Commerce for people and organizations**

By utilizing mobile commerce the user is simply and at every place and times, able to access his/her own data. The main advantage of M-commerce comparing to Ecommerce also exists in. In fact while the use of E-commerce is provided only when the user is at his/her own home or workplace or in any other location he/she has to access media such as, Internet, TV. M-commerce merely need the Mobile-phone. However this doesn't bear the meaning that M-commerce is limited to ordinary applications like reading E-mail or reporting. Within the pass of time the services and ample abilities of M-commerce are getting more popular and more complete than the E-commerce. Generally, M-commerce has several major advantages to consumers are :

**Context-specific services –** M-Commerce makes it possible to offer location based services, which are specific to a given context (e.g. time of the day, location and the interests of the user).

**Time-critical situations -** The ubiquity and immediacy of Mobile Commerce allows user to perform urgent tasks in an efficient manner, irrespective of his current geographic location.

**Spontaneous decisions and need-** Spontaneous needs are not externally triggered and generally involve decisions that do not require a very careful consideration, e.g. purchase decisions involving small amounts of money.

**Efficiency increase -** Mobile Commerce helps increase the productivity of the workforce by increasing the efficiency of

their daily routines. Time (employees) can use dead spots in the day, e.g. during the daily travel to and from workplace, more effectively.

**Factors affecting MEC applications and services**

Hand held terminals can be considered as access devices to Internet. As such, they don't change the nature of Internet applications. However, services and applications successfully being offered over the Internet (e.g. financial or travel services), in order to have similar success in MEC, they need to take into account the peculiarities of mobile wireless computing and wireless devices analyzed before as well as the different needs of mobile users and the different usage of hand held devices: users need location-based services (e.g. maps, nearby restaurants) as well as personalized information and services, e.g. time management facilities and access to personal information in an easy and secure way. Furthermore, the use of mobile terminals makes them an ideal candidate for becoming an electronic wallet. Security issues are essential and compromises have to be made between the provided security and functionality. Figure 1 shows the impact of various factors on MEC applications and services.

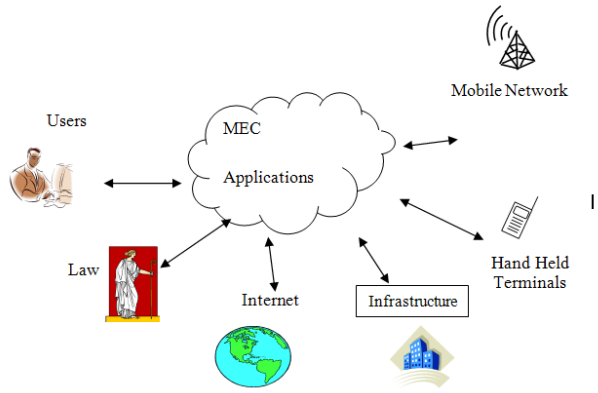



Figure 1. Factors affecting MEC applications and Services

As it can be seen, most of the arrows are bi-directional. This is because there is influence on both sides. More specifically, limitations of Mobile Networks (e.g. relatively low bandwidth) or of hand held terminals (e.g. small screens) impose certain requirements on MEC applications and services and, at the same time, limitations of existing applications demand further improvements from networks and hand held terminals. The arrow from mobile network infrastructure on hand held terminals denotes that hand held terminals, in order to exploit the advantages offered by advanced network technologies (e.g. WAP) have to change accordingly.

Existing legislation imposes constraints on certain aspects in MEC. For example, in some countries privacy protection doesn't allow the users' location to be given to service providers. On the other hand, the peculiarities of MEC (e.g. the fact that the user can close a contract very easily and in any country) require certain legislation to be defined in order to support e-commerce (e.g. out-of-court dispute settlements or electronic cancellation of contracts). And, of course, user's needs influence the development of MEC applications and services. At the same time, the offered applications and services have an impact on users' needs, e.g. since the user enjoys the benefits of location-based services and can, for instance request guiding instructions to reach a place, s/he will also demand to have location-based services in his/her language when s/he is abroad that can be accessed in a familiar way.

**M-commerce Security Concerns**

M-Commerce is bringing together two technologies, wireless communication and traditional E-Commerce, with a history of security problems. Coupled with the convergence of voice and data communications, interconnection with external data networks and issues surrounding the transactions themselves, the potential risks are very high [3]. There are three basic security components in M Commerce:

(a) *Transaction:* protecting the transaction parties and their data by providing an acceptable level of security,

(b)*Information:* protecting valuable and sensitive information about customers, and

(c) *Infrastructure:* protecting the network infrastructure from attack.

Wireless communications make physical eavesdropping almost undetectable [13]. Similar to wired communication, wireless communication also needs three basic security requirements: (i) confidentiality- information is disclosed only to legitimate entities or processes, (ii) integrity- unauthorized modification of information is prevented, and (iii) availability- authorized entities can access a service provided they have appropriate privileges. M-Commerce needs several layers of security: (i) device security, (ii) language security and (iii) wireless security.

**1 Device Security**

Within the design of mobile devices, there are a number of high quality security features. The most important of these are: (i) a built-in password mechanism which will lock after several mistyped attempts and (ii) an industry approved, tamper-proof smart card, known as Subscriber Identification Module (SIM) card. The SIM card and the mobile device are always stored together and the device is an every day utility object that is easily lost or stolen. Time-out and key-locks are often not used on phones. This means that as long as the phone remains turned on the strong password system will be bypassed. All WAP data, in some popular handsets, is stored in the phone's memory, not in the SIM; this will include login and password information. These features certainly diminish the security of the mobile phone. The SIM card used in mobile devices are *de facto* microprocessor and they can be used to facilitate mobile commerce. Gemplus SIM cards features a digital signature and public key encryption [14] and the technology is embedded in the card. In May 1999, Motorola, jointly with Identix, a biometrics company, developed fingerprint scanning devices, called the DFR 300 that is 4.5 milli- meters thick [2]. This scanning device can now be incor-porated into the HWDs.

**2 Language Securities**

If special purpose M-Commerce software, such as a stock trading application, is to be deployed on mobile The Fourth International Conference on Electronic Business (ICEB2004) / Beijing 809 devices, then Java is the recommended

language to be used as the deployment language on the HWDs. By using Java, the amount of software that needs to be changed in order to adopt the application to various mobile platforms is minimized. Feasible Java execution environments are available for PDAs, Smart phones, Communicators (such as Symbian), laptops, and other platforms. Maffeis [6] also recommended using server side Java technology, such as the Jave-2 Enterprise Edition (J2EE) platform, in the data center. This allows for shorter time-to-market and avoids vendor lock-in.

**3 Wireless Securities**

**3.1 WAP Security**

WAP (Wireless Applications Protocol) is 'an open, global specification that empowers mobile users with wireless devices to easily access and interact with information and services instantly.' WAP is currently the only publicly available solution for wireless communication and enables M-Commerce where Internet data moves to and from wireless devices. WAP enabled phones can access interactive services such as information, location-based services, corporate information and interactive entertainment. WAP is targeted at various types of HWD and Bluetooth enabled mobile phones. WAP 1.x security uses the Wireless Transport Layer Security (WTLS) protocol. This protocol is the WAP equivalent of Secure Socket Layer (SSL) and it provides authentication, encryption and integrity services. WTLS has three levels, all have privacy and integrity: (i) *Class- 1* has no authentication (anonymous), (ii) *Class-II* has server authentication only, and (iii) *Class-III* has both client and server authentication. WTLS supports some familiar algorithms like Diffe-Hellman, RC5, SHA-1, and IDEA. It also supports some trusted methods like DES and 3DES, but it does not support Blowfish and PGP [9]. The WAP gateway is software that runs on the computer of the Mobile Service Provider (MSP). Thus sensitive information is translated into original unencrypted form at the WAP gateway [5]. This problem is known as WAP gap. Public key cryptography (PKC) is used to exchange a symmetric or private key using certificate and then all transmission is encrypted.

**4 Wireless LAN (WLAN) Security**

**4.1 IEEE 802.11b**

The WLAN standard IEEE 802.11b provides a mechanism for authentication and encryption. It provides a maximum of 11 Mbps wireless Ethernet connections using the band at 2.4 GHz. 802.11b security features consists of security framework called Wired Equivalent Privacy (WEP). WEP is based on RC4, a symmetric stream cipher. It has a pseudo-random number generator, whose output is XORed to the data. WEP can use 40 or 128 bits key size. However, using a 128 bits key size, 802.11b throughput drops much due to heavy calculations. In August 2001, RC4 was announced to be broken and can be cracked in less than half an hour. Consequently, WEP can be broken. WEP with 40 bits key size can be broken in real time.

**4.2 Bluetooth**

Bluetooth technology, developed by Ericsson in 1998, is used to connect different HWDs and provides a method for authenticating devices. Device authentication is provided using a shared secret between the two devices. The common shared secret is called a *link key*, generated from PIN. This link key is established in a special communication session called *pairing*. All paired devices share a common link key. There are two types of link keys: (i) *unit keys* and (ii) *combination keys* [17]. The link key is a 128-bit random number. A device using a unit key uses the same secret for *all* of its connections. Unit keys are appropriate for devices with limited memory or a limited user interface. During the pairing procedure the unit key is encrypted and transferred to the other unit. Only one of the two paired units is allowed to use a unit key. Combination keys are link keys that are unique to a particular pair of devices and they are only used to protect the communication between these two devices. Clearly a device that uses a unit key is not as secure as a device that uses a combination key. Since a unit key is common to all devices with which the device has been paired, all such devices have knowledge of the unit key. Consequently they are able to eavesdrop on any traffic based on this key. In every Bluetooth device, there are four entities used for maintaining the security at the link level: (i) the Bluetooth device has an IEEE defined 48-bit unique address, (ii) a private authentication key which is a 128- bit random number, (iii) a 8-128 bit long private encryption key, and (iv) a random number, which is frequently a changing 128-bit number that is made by the Bluetooth device itself [12]. The security algorithms of Bluetooth are considered strong. Bluetooth standard does not use the RC4 cipher; rather it uses the E1, a modified block cipher SAFER+. No practical direct attack has been reported.

**Trends of M-Commerce in India**

Indian M-Commerce Will Reach $19 Billion By 2019:

India's online retail market is on the radar of global investors and eCommerce players, which have announced investments topping $3.6 billion in the past three months, including $2 billion in Amazon, $1 billion in Flip kart, and potentially $650 million in Snap deal. Growth in India's online retail market is powered by its fast-growing smartphone penetration, as customers are increasingly using their mobile phones to buy products online. More than half of Snap deal's and Flip kart's sales and nearly 35% of Amazon's traffic come from mobile in last few months.While India is still a small eCommerce market, it's growing at the fastest rate in the Asia Pacific region. According to Forrester's Asia Pacific Online Retail Forecast, 2014 to 2019, India will have 125 million online buyers by the end of 2019. Forrester expects mobile to overtake PCs in 2016 in terms of sales and reach $19 billion by 2019. Key factors driving M-Commerce growth include customer demand and investment from key players:

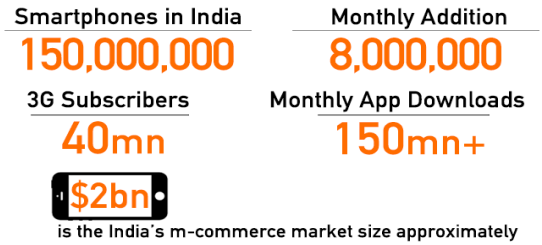
- **More people from tier two, three, and four cities are buying on mobile.** Nearly one-third of India's 1.2 billion people lives in tier one through tier four cities — the near-term addressable market for eCommerce companies. Only 8% of the populace lives in the top eight tier one city, where eCommerce penetration is already high. Other cities face low PC and broadband penetration but also have fewer brick-and-mortar stores, allowing eCommerce to fill the gap. Smart phones are enabling ecommerce in tier two, three, and four cities where broadband

penetration is very low. Mobile phones are the primary purchasing channels in tier three cities, regardless of how frequently a consumer purchases. The use of PCs for online buying is lower in tier three cities than in other tiers; around 62% of online fashion store Jabong's recent sales and 45% of the revenues of Myntra (acquired by Flipkart in May 2014) come from physical stores in tier two and tier three cities. We expect people living in tier four cities (16% of India's population) to behave similarly to those in tier three and adopt eCommerce via mobile [15].

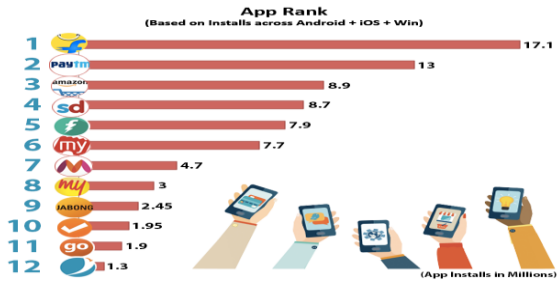
- **Vendors are investing more in mobile platforms.** Key market players including Amazon, Flipkart, Jabong, and Snapdeal have already promised increased focus on and investment in the mobile space. Paytm is looking to raise $200 million to become full-fledged mCommerce company. Paytm aims to process 1 million mobile orders per day by 2016, up from around 320,000 currently. Another player, Freecharge, also raised $33 million to build an offline-to-online advertising platform to tap the growing mCommerce market.

Visualised: India's Mobile Commerce Growth In 2014 has been a landmark year for Indian e-commerce with billions of dollars invested across top commerce players. Most of this investment has gone into the development of infrastructure, marketing & manpower. Interestingly, most of the marketing money is being spent to grow the mobile base. Smartphones and "Mobile Only" Internet users are growing rapidly and India is expecting to double its base of smartphones and mobile internet subscribers by the end of 2015.

Let's take a visual look at how some of the top mobile commerce apps of India grew in the year 2014, which also points towards the overall growth of mobile commerce in India[16].




.




For this article, I decided to include 12 popular apps from diverse commerce categories like Shopping, Travel and Online Recharge. Most of the data presented here has been compiled using various 3rd party services like AppAnnie, XYO.net & PlaystoreAPI which offered good insights on the install base and average monthly growth.Now let's have a look at the install base of all the 12 apps being featured in this article. Clearly Flipkart with over 17mn base leads the chart, followed by Paytm

Install base calculated based on the data available on Xyo.net coupled with my own secret formula taking into account the install bracket, total ratings, number of reviews and rank over time in 2014.

A Flipkart's app was available on Android in year 2012 but the real push came in the year 2014 when they launched the TV campaign for promoting the mobile app specifically. In (.12 million to 1 million) October they celebrated Big Billion Day which led to strong growth followed by Mobile App Shopping Days in Dec 2014.

## IV.CONCLUSION

This paper has shown that the M-commerce market place in India has grown and is growing continually which brings both opportunities and challenges for customers, businessmen and regulators. The wide spread use of mobile devices now a day generates huge amount of revenue by reducing time and money needed for multiple purposes. It also shows the protocols that have been developed in order to make our mobile commerce safe and secure from fraud.

## REFERENCES

**[1]** Buellingen, F., M. Woerter, Development perspectives, firmstrategies and applications in mobile commerce[J]. Journal of Business Research, Elsevier Inc, 2004

**[2]** Goldman, Jeff, "Wireless Security and MCommerce", The Feature, March 8, 2001, http://www.thefeature.com/article?articleid=9862

**[3]** Messham, James, "M-Commerce Security", <http://www.tdap.co.uk/uk/archive/billing/bill(fml_0012).html>

**[4]** Efraim, T., David K., Introduction to E-commerce[M].Prentice Hall, 2002

**[5]** Juul, Niels C. and Jorgensen, N. "WAP may stumble over the Gateway", 2001, http://webhotel.ruc.dk/ncjuul/papers/wap.pdf

**[6]** Maffeis, S. "M-Commerce Needs Middleware!", 2000, http://www.softwired-inc.com/people/maffeis/articles/softwired/mcommerce.pdf

**[7]** Lee, C.W., Hu, W.C., Yeh, J.H., A System Model for Mobile Commerce[C]. Proceedings of the International Workshop on Multimedia Network Systems and Applications, Providence, Rhode Island, May, 2003

**[8]** Michael S., David S., A model for small business new technology adoption: the case of mobile commerce[C]. Proceedings of 2003 ASBE Conference, Houston, TexasMar. 5-8, 2003

**[9]** Osborne, Mark, "WAP, m-commerce and security", 2000,http://www.kpmg.co.uk/kpmg/uk/image/ mcom5.pdf

**[10]** Tarasewich, P., Nickerson, R.C., Warkentin, M., Issues in mobile commerce[C]. Communications of the Association for Information Systems, Vol. 8, 2002, pp41-64

**[11]** Varshney, U., R. Vetter, Mobile Commerce: Framework, Applications, and Networking Support[J]. ACM/Kluwer Journal on Mobile Networks and Applications (MONET), Vol. 7, No. 3, Jun, 2002, pp185-198

**[12]**Vainio, J.T. "Bluetooth Security", 2000, http://www.niksula.cs.hut.fi/~jiitv/bluesec.html

**[13]**Pietro, Robert D. and Luigi V. Mancini, "Security and Privacy Issues of Handheld and Wearable Devices", Communication of the ACM, Vol. 46(9), pp75-79, September 2003

**[14]**"PKI Moves Forward Across the Globe", Wireless developer Network, http://www.wirelessdevnet.com/channels/wap/features/mcommerce3.html