Building a Strategic m-Commerce Services Platform

STANISLAV MILANOVIC *, NIKOS E. MASTORAKIS * #

* WSEAS, Highest Institute of Education, Science and Technology
Haghiou I. Theologou 17
15773, Zographou,
Athens, GREECE

# MILITARY INSTITUTIONS OF UNIVERSITY EDUCATION
HELLENIC NAVAL ACADEMY
Terma Hatzikyriakou, 18539, Piraeus, GREECE.

Abstract: A secure, scalable mobile transaction solution over multiple Internet-enabled devices and access channels has been highlighted. The aim of this paper is to enable m-Commerce service providers – network operators, online portals, financial services organizations, leading merchants, or others – to realize the tremendous opportunity m-Commerce presents.

Key-words: m-Commerce transactions, buyer – seller interaction, mobile Internet, portal, PKI.

1 Introduction

Mobile commerce (m-Commerce) is radically improving how we shop and how we pay. The opportunity for adoption by consumers is enormous – but to date, the hype has outstripped the capability of organizations seeking to capitalize on this opportunity to deliver. The reality is that innovative organizations can drive adoption today by hiding technology complexity, and delivering convenient, secure and personalized buyer – seller interaction across all stages of a transaction [1-18]. Global m-Commerce transaction revenue is forecast to exceed $200 billion by 2005 (Figure 1). Not surprisingly, a significant number of intermediaries are now emerging to enable buyers and sellers to complete m-Commerce transactions with each other in the wireless world.

The mobile Internet – the convergence of wireless data and Internet protocol (IP) – represents a huge opportunity and m-Commerce represents the means to monetize it. Based on a value proposition of unparalleled convenience, the mobile Internet is set to surpass even the wired Internet as a medium over which buyers and sellers transact. The rapid adoption of personal computers (PC) and wireless data devices, coupled with the growing ubiquity of the Internet as a medium through which to conduct business, is significantly changing the nature of the transactions and payments upon which commerce is built.

Transactions are the next wave of the mobile Internet and for any organization having a stake in facilitating buyer – seller interaction the time to act is now.

Key to making these m-Commerce transactions successfully enhance the relationship between buyer and seller will be to ensure that the underlying facilitating technology remains invisible to both parties. For m-Commerce service providers, selecting, testing, and refining an m-Commerce offering today is critical to competitive advantage as adoption rates climb steeply. To succeed, the efforts of the service provider need to be squarely focused on delivering value-added m-Commerce services that enhance buyer – seller interaction resulting in increased dollar value and volume of transactions. Consequently, the underlying m-Commerce service delivery platform must comprise a highly scalable and secure wireless transaction enabling technology and modular delivery solution – one that provides the ability to continually
add and evolve new services and support new devices and technologies that optimize service delivery. By adopting and implementing such a platform, service providers can focus on executing their business model rather than continually struggling with technology challenges.

![Global m-Commerce transaction revenue forecast (in billions)](image)

**Source:** McKinsey & Co.

**Figure 1.** Global m-Commerce transaction revenue forecast (in billions)

### 2 m-Commerce – delivering anywhere, anytime convenience

With "Internet-ready" mobile phones shipping at a ratio of three mobile phones for every PC, the number of mobile Internet access points is growing rapidly. These new IP-connected mobile devices place the power of the Internet in the hand of the consumer, providing ubiquitous mobile access to information, content, and transactions (Figure 2).

m-Commerce services should stimulate buyers by making available context-based services, central and easily accessible sources of product and service information and shopping agents. Buyers should be directed to buy based on their preferences and interests, have the ability to find the desired product or service and to "buy now" regardless of where they are, and what device they are using. These services should also make it easy for buyers to pay using both existing and emerging payment products and infrastructure. Finally, buyers should be able to immediately receive electronic goods or services, such as tickets or entertainment receipts, as part of the fulfilment process.
Financial services have been at the vanguard of the wireless movement [19]. Not only have they moved beyond the human teller, they are now moving past more traditional convenience services such as the automated teller machine (ATM) to offer customers a vast array of e-banking services. And with the advent of wireless technology comes a demand from their customers – who are already using their personal digital assistants (PDAs), to access email – to complete their banking transactions in the same fashion. As a result, financial institutions (FIs) that fail to offer wireless e-banking services risk losing their customers to the competition and they risk losing an opportunity to deepen their relationships with customers and merchants. This migration towards wireless banking and commerce will not come without significant challenges, chief among them are security concerns.

Security is the most oft-cited reason for individuals who choose not to embrace the convenience of online shopping or e-banking. The concerns become even greater as services move from the wired desktop to the untethered portable device. It won’t be enough for financial institutions to simply assure merchants and consumers that they have a secure mobile e-Commerce infrastructure – it will be key for them to back up those claims with the proper security technology.

It is important for financial institutions and end-users alike to understand the security threats that exist in the Internet and wireless environments, and specific security safeguards to mitigate the exposure to risks. In short, they want their financial transactions to reflect three fundamental principles or goals of security:

1. Respect for privacy.
2. Protection of confidential information.
3. Assurance of business integrity.

For a wireless banking and brokerage service, this means:

- A person’s financial and personal information should never be disclosed to unauthorized parties.
- All information should be protected (e.g., encrypted) to prevent others from stealing or modifying that information.
- User identities must be verified.
- Personalized privilege and authority policies should be enforced.
- The wireless platform should leave a detailed “digital trail” that prevents repudiation – that is, to ensure transactions cannot be denied by either party.
Financial institutions and network operators have both a unique opportunity and a significant role to play in delivering secure and trusted m-Commerce services [20]. For the m-Commerce service provider, enabling secure, personalized payment completion will be critical to successfully driving an increasing volume of transactions online. As the dollar value and volume of transactions increases and the m-commerce market evolves, buyer authentication will become an even more important issue for sellers seeking to minimize fraud. This, in turn, opens the door for service providers to launch new wireless services supporting a wide range of higher value m-Commerce transactions. Ensuring strong authentication and non-repudiation through digital signatures – two key elements to taking the risk out of mobile transactions – necessitates that the underlying m-Commerce platform be robust and open enough to support a wide range of public key infrastructures (PKI). Integrating this support at the application level enables the flexible implementation of policies governing which transactions must be digitally signed by the buyer, while lower risk transactions can undergo a fast-tracked completion.

3 Objective
A principal objective was to launch an online portal providing secure personal wireless banking, brokerage, information, lifestyle and shopping services on the customer’s choice of mobile devices. The m-Commerce portal is to be available in English, German and French on several leading wireless carriers. Portal customers, using digital mobile phones and pagers, should be able to access the following services:
- Mobile Banking – view account balances, transfer money between accounts, pay bills, order checks.
- Mobile Brokerage – set-up watch lists, look-up stock quotes, trade stocks.
- Mobile Commerce offerings and Shopping – scroll through chosen bricks-and-clicks retailer Indigo’s collection of bestseller lists, and purchase books using express "buy" functionality. Airline and movie tickets ordering and making restaurant reservations.
- Mobile Lifestyle – access content such as news, weather, horoscopes, AirMiles loyalty program etc.

4 Requirements
The main requirement was to deploy a complete m-commerce service delivery platform and suite of applications that maximize m-commerce transactions and enable secure electronic payment over a wide range of channels. With the method of payment becoming increasingly electronic in nature, the ability to access easy to use, personalized payment services to complete a mobile purchase is of increasingly high importance to consumers. They are already accustomed to small-screen displays (POS, ATM, etc.) for completing retail transactions, and are requesting the convenience provided by an always-on, always-connected mobile device that let them complete payments online. Consumers also wanted to choose how to pay and in addition to secure, simple, "express buy" functionality, the m-commerce platform must provide multiple payment options including credit, debit and new electronic payment forms such as micro payments that facilitate m-Commerce transactions. This functionality must be available across m-Commerce applications and accessible from any mobile device.

5 m-Commerce Solution
Deployed m-Commerce solution was made up of a number of components separated into different areas, and managed as security zones: Access Channel Zone, Mid-tier Zone, and m-Commerce Services Zone. Each of these zones were considered a distinct trust domain with its own security policies and practices.
Device zone is comprised of the actual devices – such as a mobile phone or a PDA – the customer uses to conduct wireless financial transactions. Just as a password or personal identification number (PIN) is required when a customer conducts financial transactions through an automated teller machine (ATM) or a financial services Web site, m-Commerce Services Platform (m-CSP) users must first sign-on with their unique user ID and secret password to access even the basic m-CSP services such as news, weather and stock quotes. Credentials are once again required to access personal account data located at a financial institution.

The financial institution may additionally require another user identifier (user id) and/or some specific authentication data, such as a password or PIN, when special transactions – such as trade confirmation – are executed. It is important for end-users to remember that much like a credit card holder should immediately report a lost or stolen card to suspend the account and mitigate damages, a mobile device owner that conducts wireless e-banking should change the password or suspend the account if that device is ever lost or stolen. The financial institution makes this service available through a call center or a self-service account management Web site. In the case of passwords that have been forgotten or need to be changed, the m-CSP requires users to correctly respond to one or more personal identification questions, established at the time of initial enrollment.

Different devices have different security capabilities while some devices do not have any inherent security capabilities at all. On Palm devices using the m-CSP native client, Elliptic Curve Cryptosystem (ECC)-based algorithms enable ECC-based transport layer security (TLS) between the device and m-CSP and message verification is accomplished using secure hash algorithms. On the Palm VII device, ECC is embedded in the Palm operating system to enable secure communications between the device and Palm.net gateway. Using smart cards on GSM handsets, PKI functionality enables transaction confidentiality and digital signatures for non-repudiation and authentication.

Network and carrier infrastructure zone is comprised of the device’s network delivery and carrier infrastructure providing the
communications channel into the wireless financial services platform. Information entered into the mobile device by the end-user and, in turn, information received from the financial institution passes through a secure communications channel that ensures both confidentiality and data integrity. Generally, sensitive information is encrypted for communication using a strong 128-bit cipher. This is the strongest cryptographic technology exportable for commercial use by financial institutions.

Customers using Palm devices for communicating with a financial institution via the m-CSP have their information carried over a channel reserved for Palm devices. This channel uses the Internet Transport Layer Security (TLS) protocol with Elliptic Curve Cryptosystem (ECC) public-key technology from Certicom Corp. This Internet standard compliant implementation is a variant of the well-known Secure Sockets Layer (SSL) handshake protocol, but uses 163-bit ECC keys that are equivalent in strength to 2048-bit RSA keys.

Messages are encrypted using the industry standard RC4 cipher algorithm with a 128-bit shared-secret session key negotiated using an ECC variant of the Diffie-Hellman key exchange protocol (ECDH) when the connection session is initially established. Additionally, each transaction communicated on the Palm client channel contains a message authentication code (MAC) used to verify its origin and detect whether it has been changed in any way. This MAC is constructed using the Secure Hash Algorithm (SHA-1) in accordance with the HMAC Message Authentication standard (RFC 2104). Palm VII devices provide DESX encryption for communication between the device and the Palm.net gateway. The shared secret session key is established using Certicom’s One Pass Protocol. Messages destined for the m-CSP are decrypted and then re-encrypted at the Palm.net server for communication via a 128-bit SSL connection established using 1024-bit RSA keys and digital certificates.

Messages are communicated securely between WAP enabled devices and the WAP gateway using the Wireless Transaction Layer Security (WTLS) protocol as defined in the Wireless Application Protocol (WAP) standards. Messages destined for the m-CSP are decrypted and then re-encrypted at the WAP gateway for communication via a 128-bit SSL connection established using 1024-bit RSA keys and digital certificates. Mobile phones enabled with Phone.com’s UP.Browser provide 128-bit encryption via the industry standard RC5 cipher for communication on the over-the-air link between the handset and a Phone.com UP.Link gateway server at the mobile operator’s facility. Messages destined for the wireless financial services platform are decrypted and then re-encrypted at the UP.Link server for communication via a 128-bit SSL connection established with mutual-authentication using 1024-bit RSA keys and digital certificates.

Although the focus thus far has been on wireless access to financial transactions, it is important to note that the m-CSP also provides security measures for end-users who may be e-banking from their home PC with conventional HTML Web browsers. A secure connection between the browser and the m-CSP may be established using the standard 128-bit SSL protocol.

The m-CSP has also been enabled to use a public key infrastructure (PKI) with digital certificates for end-user authentication. Public keys and digital certificates are required by m-CSP servers in order to establish secure connections. In particular, the channel server proxy for Palm devices has ECC keys needed for the ECC-enabled TLS (eTLS) protocol. An eTLS key manager tool is provided to issue key-pairs and digital certificates for use on such servers. The SSL servers require digital certificates issued by a certificate authority (CA) – either a trusted third party, such as VeriSign or Certicom, or a CA operated by the host financial institution using a product from, for example, Baltimore Technologies, VeriSign, or Entrust.

- Mid-tier zone is where the core of the financial institution’s wireless solution resides, including its mid-tier transaction system platforms, network infrastructure and content aggregation services for delivering stock quotes, news, weather and other
lifestyle information to supplement the user experience. This zone is deemed to be trustworthy – assuming implementation of recommended policies and best industry practices for ensuring operating system platform, network, and physical security, and limiting access to specific authorized individuals. Countermeasures have been implemented to guard against interference using intrusion detection; denial of service using firewall configurations and applying known and current information and software solutions to guard against such attacks; message modification using integrity checks (using hashing algorithms or message authentication codes); and channel spoofing.

PKI Gateway is an open and standards-based PKI solution for the financial services industry able to interoperate with a wide range of existing PKI technologies and certificate authorities (CAs). As various kinds of devices have different security capabilities, the PKI Gateway needed be capable of handling these differences by supporting various public key cryptosystems, certificate formats and management protocols and mechanisms. It must be able to support and route a certificate request from a client device to CA/RA regardless of the CA/RA product and technology used in the PKI.

- m-Commerce services zone comprises the financial transaction processing systems – hosted at the banks, brokerages, merchants or other financial service providers – and the communication channel to those systems from the mid-tier environment to the Open Financial Exchange (OFX) servers, which provide message-based access to the financial institution’s systems of record. Depending on the network topology, such a zone might be more or less trustworthy. For instance, if this zone is wholly contained within a financial institution’s secure internal environment – implying collocation with an m-CSP mid-tier environment operated by the financial institution – then it can be considered to be highly trustworthy. However, when an m-CSP gateway is not co-located with a financial institution’s back-end servers, transactions must be carried over the Internet – making part of this zone much less trustworthy. Two security options are available to mitigate the risks in this latter circumstance:
  1. The m-CSP protocol gateway should be configured to use a secure RSA-based 128-bit SSL connection.
  2. A secure leased-line with virtual private network (VPN) firewall routers – should be installed between the mid-tier and the m-Commerce services zone.

6 Conclusion

The rapid proliferation of many new forms of mobile Internet devices is providing new opportunities for commerce transactions. Increasingly, these handheld devices are being designed for m-Commerce transactions, and m-Commerce is a natural extension and complement to the current Internet shopping experience that has seen rapid growth on the PC channel.

Deployed end-to-end solution delivers simple yet compelling m-Commerce applications while leveraging existing payment networks and systems and enabling secure mobile purchasing. Service provider has leveraged robust, future-proofed m-Commerce platform technologies that enabled the delivery of value added m-Commerce services today, while at the same time has provided scalability and flexibility to continually exploit the unique advantages of the wireless channel and drive m-Commerce adoption.

References:


