Business solutions for mobile e-commerce

Olle Källström

Demand is building for consumer-to-business mobile e-commerce that will enable consumers to use mobile phones to perform financial transactions in a secure manner. Mobile e-commerce literally puts Internet-based purchasing power into the hands of consumers, allowing a degree of personalization never before seen. It opens up a new path to the market for today's content and service providers and enables the creation of an array of services native to mobile communications. In all likelihood, mobile e-commerce solutions will generate a variety of totally new applications in the same way as the mobile Internet—which while an extension of fixed Internet has also given rise to completely new applications driven by mobility.

The author describes the prerequisites for this market and the value-added solutions that mobile telephony services can contribute to the world of Internet e-commerce. He explains how end-users, service providers, merchants, and network operators are likely to benefit from mobile e-commerce solutions—like Ericsson's Mobile e-Pay combined with other solutions—that will give rise to new services and business opportunities.

Both the Internet and wireless systems are expanding at a rapid pace. In the overlap of these growth areas, we find the mobile Internet. One of the most interesting business opportunities here is mobile electronic commerce (e-commerce). In the emerging global digital economy, mobile e-commerce will provide secure financial transaction services for consumers anywhere, anytime. Initially, mobile e-commerce services will be adapted from conventional Internet services extended to mobile phones. Later, new services will be based on the unique demands of mobile users.

BOX A, ABBREVIATIONS

3DES	Triple DES
API	Application program interface
CA	Certificate authority
DES	Digital encryption standard
GPRS	General packet radio service
GSM	Global system for mobile communication
HMAC	Keyed-hashing message authentication code
HTTP	Hypertext transfer protocol
IP	Internet protocol
IPP	Internet payment provider
ISP	Internet service provider
MAC	Message authentication code
MD5	Message digest 5 (algorithm)
MSISDN	Mobile station integrated services digital number
OA&M	Operation, administration and maintenance
PIN	Personal identification number
PKCS	Public key cryptographic standard
PKI	Public key infrastructure
RSA	Rivest-Shamir-Adleman
SAT	SIM application toolkit
SHA-1	Secure hash algorithm 1
SIM	Subscriber identity module
SMS	Short message service
SMSC	SMS center
SSL	Secure socket layer
TDMA	Time-division multiple access
WAP	Wireless application protocol
WIM	Wireless interface module
WPKI	Wireless PKI
WTLS	Wireless transport layer security

The roots of e-commerce

Many people regard e-commerce as buying and selling products and services over the Internet, but it has many more aspects. From its inception, e-commerce consisted primarily of purchase transactions and the transfer of funds over computer networks. Now it has grown to include the buying and selling of new commodities such as electronic information. Thus, the opportunities for companies seeking to take advantage of the capabilities of e-commerce are greater than those offered by merely moving our present ways of performing commercial transactions to electronic networks.

E-commerce has its roots in online transactions between large corporations, banks, and other financial institutions. But small companies are just as capable of conducting business online as their biggest competitors. Businesses of all sizes are finding that they can lower their e-commerce costs, either by replacing other networks with the Internet, by using it as another communications medium, by converting their business data to digital form, or by incorporating Internet functions into their business practices. Whatever the case, the rapid growth in buying and selling over the Internet by private individuals has only recently attracted the attention of the business community and mass media.

Given the transportation systems of today, the world is the market for anyone with a product—provided potential customers are aware of the product and have reliable methods for ordering and paying for it. The Internet and e-commerce have finally given us the information technology systems that can interact with and exploit the global transport systems for delivering products worldwide. The concepts *time of day* and *location* have lost their importance; instead, *online access* and *availability* are the key factors for success.

A new business paradigm, spawned by the emerging global digital economy, promises explosive growth in electronic commerce on the Internet. In a global market, competition is widespread. Those companies that can cultivate the global marketplace by using the Internet effectively will eventually emerge as winners. We see this today in portals like AOL and Yahoo, and sites like Amazon and eBay.

Electronic marketplaces

The explosion of e-commerce activity is leading to the creation of electronic marketplaces. These are made up of digital virtual businesses that band together in an open but secure environment to interact with each other and customers. On the Internet today, we already see

- virtual superstores;
- electronic storefronts for existing services;
- auctions and flea markets;
- virtual order centers;
- intranet-based electronic business communities; and
- virtual trading marketplaces.

These new digital marketplaces have one thing in common: they are closed in the sense that they are run by one company and include handpicked business partners or loyal online consumers who are found at a single website. As the e-commerce business matures, new forms of the open electronic marketplace will evolve, confirming the Internet's true nature as a global marketplace.

Thus, e-commerce is part of a larger process of change that is engendering a completely new market environment and new business relationships. The new, electronic economy will be as different from today's industrial economy as the latter was from the economy of agrarian societies.

Payments over the Internet

The market for inexpensive digital goods and services has not grown as much as predicted. It is hard to tell whether this is due to a lack of demand or a lack of secure and commercially viable methods of making micro-payments. Nonetheless, the growing use of the Internet for trading in goods and services has heightened the need for robust payment solutions. During the past few years, many initiatives have been adopted to develop and market entirely new payment methods and to adapt existing payment systems to the Internet. The main focus of development for these systems has been on security.

In the past, systems devised for both micro-payments and regular transactions often required customers to download and install software in their computers and to register with the system offline—for example, by letter or fax. For payment to be effected, both supplier and customer had to be connected to the same system or company. Today, most systems of this kind have disappeared or are in decline.

In the global market for online payments (especially in the US), payment by credit and charge cards (SSL-protected or otherwise) has now become the most common method of payment on the Internet, despite the fact that the seller cannot verify the customer's possession of the card or establish the customer's identity by the usual methods (a signature or photo ID). If the customer refuses to acknowledge the transaction, the seller has the burden of proof, because the customer's signature cannot be taken as evidence of approval. Consequently, enterprises with online sales anticipate fraud as part of their overhead. Many selling enterprises prefer cash on delivery (COD) payment or purchase orders, instead of completing the transaction online.

Notwithstanding, card payments dominate all other methods of payment. One reason is that international debit and credit cards are widely current, with more than a billion cards in circulation worldwide. No additional enrollment or connection is needed. Consumers do not need to install special software and they are familiar with this method of payment.

Figure 1
Mobile e-commerce is an "anywhere, anytime" sales channel that puts purchasing power directly into the hands of the consumer.

Now that the market for Internet e-commerce and online transactions has expanded and matured, the focus of payment solutions has shifted from the technology to the markets, and from security to user-friendliness. As a result, companies have realized that it is often easier to start with the software and means of payment already in use by customers than it is to develop entirely new solutions.

Companies who use the Internet for e-commerce no longer view it as a pilot medium but rather as a key sales channel. Consequently, these companies' choice of an e-commerce system will depend on whether it can reuse or recycle content from other sales channels and whether profit from e-commerce sales will outweigh the expense of introducing and operating the system.

Moving e-commerce to the mobile network

As trade over the Internet increases, the next logical step is to support e-commerce solu-

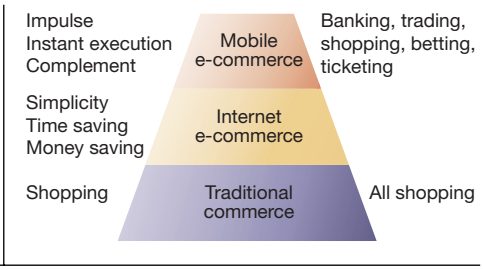


Figure 2
Comparison of traditional and online commerce and mobile e-commerce.

tions on mobile phones. WAP technology and GSM, TDMA and third-generation systems have several strengths in common: a wireless global footprint, Internet connectivity, and reliable and secure transactions. These strengths make them the ideal technological foundation for mobile e-commerce. Several manufacturers have already announced that they will market solutions that are optimized for mobile e-commerce using WAP technology.

Mobile e-commerce will complement today's Internet e-commerce by providing a secure means of financial transactions. Consumers will come to regard their mobile phones as the preferred instrument for making payments or financial transactions. Wireless technology will deliver e-commerce into consumers' hands.

Mobile e-commerce applications will stimulate end-users to make impulse purchases and to perform other transactions instantly. Such transactions will serve as a complement to traditional commerce and Internet e-commerce. Figure 2 shows the relationship between traditional commerce, Internet e-commerce and mobile e-commerce.

Early in this millennium, a significant proportion of mobile phone subscribers around the world will use mobile e-commerce applications. In some cases, these applications will be integrated into normal voice services; in others, they will be dedicated value-added solutions.

Mobile e-commerce solutions can be seen as solutions that enhance business-to-consumer trading over the Internet. They should be seamless and invisible to the end-user. They must also support any type of mobile Internet application that requires financial transactions. End-users should not have to know anything about how the system actually works. Instead, they should be able to rely on their mobile phones to execute payment.

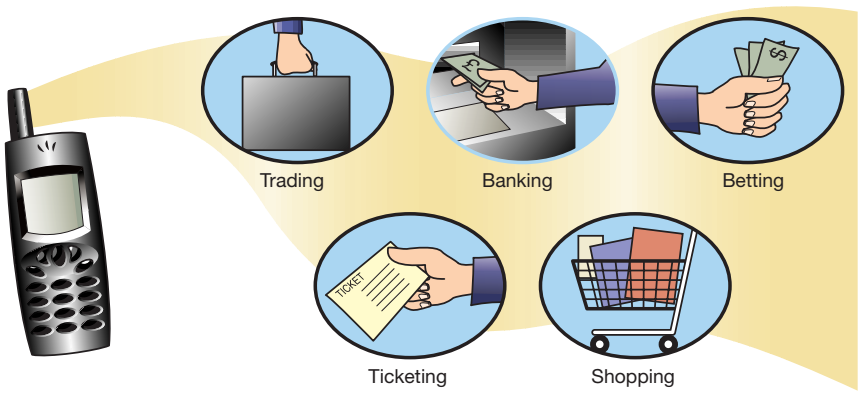
From the end-user's perspective, mobile telephony adds value to Internet e-commerce in two ways: through mobility and through the diversity of terminals. Wireless systems allow users to access services practically anywhere. Also, thanks to the widespread distribution of mobile phones, small handheld devices (such as GSM phones that contain a keypad, display, and card reader with SIM smartcard capabilities) should achieve a much broader installed base than personal computers (PC). Consequently, end-users gain at least four major benefits:

- convenience—end-users always have instant access to financial services, to make e-commerce payments anytime, anywhere;
- flexibility—users can choose the method of access and payment depending on their individual requirements;
- secure transactions—mobile terminals are reliable devices that ensure a high level of security for financial transactions; and
- familiarity—mobile phones are tools that can be personalized to present information in the format preferred by the user. Further development of the phone user interface will offer improved service interaction and extend this interaction beyond what can be achieved with today's plastic cards.

Incumbent mobile operators who face the threat of competing networks can use mobile e-commerce solutions to retain key business subscribers. At the same time, new and established operators can use these solutions to target new segments and users with sophisticated requirements.

The mobile e-commerce marketplace promises to become highly competitive.

Figure 3
The five prime categories of mobile e-commerce: trading, banking, reservations and ticketing, shopping, and games and betting.



Operators in many countries already have many value-added services in place, and competition will intensify as the roll-out of mobile data networks continues. Most of the new services will be offered by various providers of content or services. And some mobile operators are likely to offer bundled services.

As competition intensifies, operators will need to define their position more clearly and approach their market more aggressively. As operators struggle to win market shares, their interest in market segmentation will increase. Finally, as subscriber volumes grow, new end-user segments—each with different needs and demands—will be the target of focused marketing.

Mobile e-commerce and the wireless wallet

Mobile e-commerce can be offered as an extension to Internet e-commerce by introducing features for mobility and the "wireless wallet" concept.

Mobile e-commerce will deliver the goods to consumers' handsets using wireless technology that turns a mobile phone into a wireless wallet. This application can be located on an individual computer terminal and in a service provider's mobile network domain (or both). Wireless wallets will contain digital versions of what we might carry in a conventional wallet: electronic money (virtual cash), reference pointers to bank accounts, credit card numbers, certificates with digital signatures, personal data and settings, customer bonus points, tickets, and so on.

We define mobile e-commerce as a value-added service that enables end-users to conduct reliable, secure financial transactions that involve trade or payment. We also include e-banking and e-brokerage applications in our definition. Mobile e-commerce services can be classified into categories such as banking, trading, reservations and ticketing, shopping, and games and gambling (Figure 3).

Ericsson offers mobile e-commerce packages for mobile banking, mobile trading, mobile ticketing, mobile shopping and mobile betting. Each package can provide functionality for specific end-user services and applications (Figure 4).

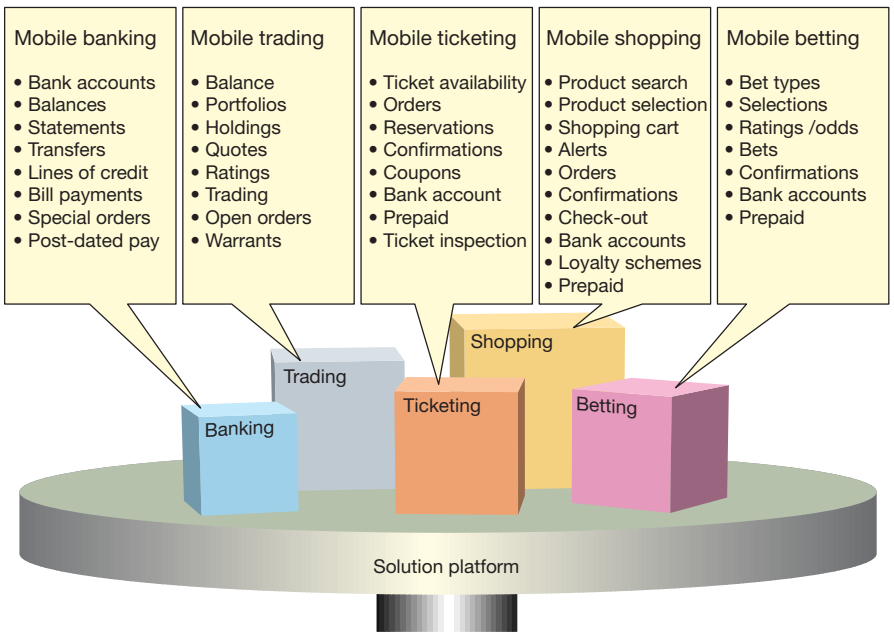


Figure 4
Solutions platform for mobile e-commerce applications.

Banking

Banking service concepts, which are an extension of Internet banking (or home banking), allow customers to use digital signatures and certificates

- to manage personal account information (account history, transfers);
- to transfer funds in bank accounts or prepaid accounts;
- to receive alerts regarding bank information or payments due; and
- to handle electronic invoice payments.

Each of these services is performed from the handheld unit and has secure end-to-end access.

Trading

Trading and brokerage applications consist of general real-time information, such as stock quotes, notification of events, portfolio management assistance and confirmed trading orders using digital signatures.

Ticketing

An electronic ticket—for an event or travel—results from transactions that involve booking, purchasing, invoicing, payment, and receipt. Optional service delivery could supply "virtual" tickets. These could be used

with a wide range of businesses: airlines, railways, mass transit, tollway authorities, theaters, sporting event organizers, theme parks, and so on.

Shopping

Shopping applications will enable regular Internet e-commerce via a mobile phone; that is, the booking and ordering of, and paying for, physical goods and services from e-shops, virtual malls and portals. Another possible use is the confirmation of payment for goods in the physical world; for instance, in shops where the user interacts directly with a cashier or a vending machine.

Games and gambling

One of the more appealing groups of applications for mobile e-commerce is likely to be entertainment. The service provider will supply a means for users to pay or sign contracts electronically. This might involve the use of payment or charging mechanisms, such as prepaid games, or direct charging via the user's phone bill. All manner of gambling is possible with pay-per-game or betting features. Online games, adventure games, and other services with pay-per-game features should also port well to mobile e-commerce.

Prerequisites for the market

The market needs a high-use penetration of mobile telephony and the Internet as well as broad acceptance of e-commerce. Indeed, Internet maturity in each local market is a key enabler for e-commerce. As with any innovation, customers must also demand new services; that is, the market should have a sufficient proportion of early adopters.

Ericsson's applications and solutions address the new end-user segment represented by an Internet generation, which we refer to as *pioneers and achievers*. These users are generally young but experienced users of mobile phones; they are accustomed to shopping online; and they have a stable income and their own mobile phone subscriptions. They also use mass-market consumer services—including personal financial services—and demand access to personal information and applications. End-users with this profile, who are eager to use new products and willing to pay for them, will constitute the market that is ready for mobile e-commerce.

Players in the market will have to focus their attention on potential key success factors. Up to now, mobile operators have usually focused on the subscriber base, attracting new subscribers by subsidizing packages and offering low-cost subscriptions. However, in some markets we can already see operators shifting their focus to services and targeting specific end-user segments. In the future, we will probably see even more of these targeted efforts by mobile operators and new service providers.

Mobile e-commerce services will evolve first in the mature GSM markets. One key component and advantage of GSM systems compared with other wireless standards (TDMA, CDMA and PDC) is the subscriber identity module (SIM), which enables tighter application security for financial transactions.

For service providers, the most interesting markets for mobile e-commerce services are those with a high degree of IT maturity and a deep penetration of mobile services. This puts Scandinavia and certain countries in northwestern Europe, such as the UK and the Netherlands, at the top of the list. North America, South Africa, Singapore, Hong Kong, Australia, and some parts of the Pacific Rim are also promising markets. Another main market (non-GSM mobile standards) with outstanding potential is Japan.

Immediate future of the market

The world of telecommunications is changing, and new players are entering the market to compete with traditional players. The market for mobile e-commerce is just opening up, so there is little real competition as yet. However, activity is increasing, and several companies have announced products in the pipeline. These include mobile e-commerce products and technologies to be supplied by Ericsson, other wireless system vendors, specialized companies, and smartcard companies. The market for mobile e-commerce is expected to take off in earnest around 2001, but the scenario is closely linked to predictions of a boom in Internet e-commerce and the further evolution of the mobile Internet.

Just as big investments are currently being pumped into Internet retailing, the same can be expected in mobile e-commerce. Now is the perfect time for vendors and operators to take the lead by investing in functionality and establishing their profile. The high-end segment of the market,

BOX B, THE E-COMMERCE TIMELINE

1999
E-commerce on the Internet increases. Business-to-consumer commerce reaches beyond early adopters. Business-to-business e-commerce achieves substantial volumes in certain companies.

2000
Initial signs of the explosion of business-to-consumer e-commerce, to continue the following two years.

2002
Consumer-to-business e-commerce is accepted and forces companies overall—including those who are not IT-savvy—to offer e-commerce services.

2005
E-commerce is a natural part of our society, integrated into all facets of day-to-day communications.

Reasons for the explosion of e-commerce in 2000–2005:
- Sufficiently improved infrastructure (commerce, communications)
- Deregulation
- Integration of e-commerce into existing systems
- Generations X and Y enter the workforce
- Merchants learn how to sell electronically
- Inexpensive access devices available (USD 100–200)
- New distribution companies in place

which will see the roll-out of WAP-enabled handsets, will be a driving factor. Figure 5 shows forecasts for the reach of wired and mobile e-commerce.

Ericsson supplies mobile e-commerce application products (for transferring, organizing and presenting digital information) that are mainly directed toward the consumer-to-business market. In addition to being independent of wireless transport services, the products

- promote the evolution of wireline consumer-to-business Internet e-commerce services into wireless;
- exploit the market by expanding today's value-added services to include the wireless wallet concept for managing money in a mobile context;
- promise increased profitability for mobile operators and providers of e-commerce services, such as Internet payment providers (IPP);
- target the banking and financial services market; and
- cater for new wireless Internet service providers (ISP) who host or own merchants and content providers.

Ericsson aims to provide solutions for three customer categories: operators, service providers and IPPs. Each one of these categories may be active in local (or national), geopolitical or global markets. However, they must have the drive to maintain and expand their existing customer bases, to reach out through new mobile channels, and to set up and maintain loyalty programs.

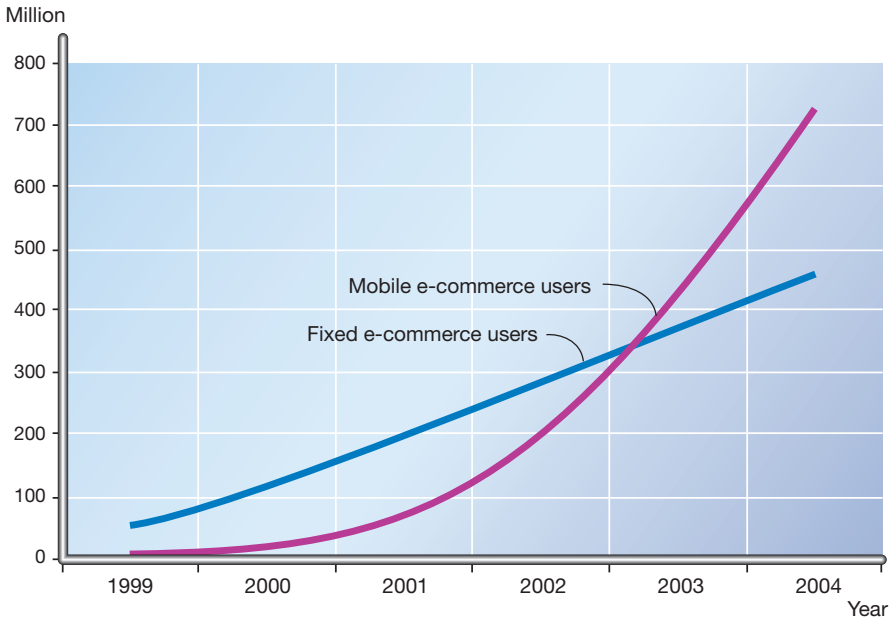


Figure 5
Forcast of users of mobile and fixed e-commerce (Source: ARC Group, Intelligence).

Applications for mobile network operators

Operators who are interested in mobile data communication make up one of the main target groups for mobile e-commerce. The solutions Ericsson offers are not infrastructure; they are application-enabling services and servers that are independent of the underlying network design. Ericsson has a complete portfolio for providing enhanced value-added services, such as end-to-end application security for financial transactions and payments.

By offering mobile e-commerce services, mobile operators, ISPs and other service providers will be able to share in the overall rapid growth of e-commerce. They will discover new business opportunities that can help them to grow and increase revenues and profits. Operators and service providers alike can create flexible charging options that allow users to pay, via their mobile phones, any amount for any service. Mobile e-commerce capability will help these organizations to position their mobile services as the best way of gaining access to goods and services, anytime, anywhere. And for those who are among the first in each market to offer these services, competitive advantage can be won through establishing a leading-edge image.

Benefits for mobile operators

Mobile e-commerce extends the wireless market beyond voice, thus enhancing the value of the operator's mobile network and terminals. New types of application will expand traffic and revenue sources for wireless operators. Mobile e-commerce is an important data application driver for the wireless application protocol (WAP) and general packet radio service (GPRS). It will help operators to build loyalty, reduce churn and differentiate services. Mobile e-commerce will also enable operators to reinvent their business by assuming new roles that broker e-commerce services.

Similar benefits apply to service and content providers, regardless of whether mobile

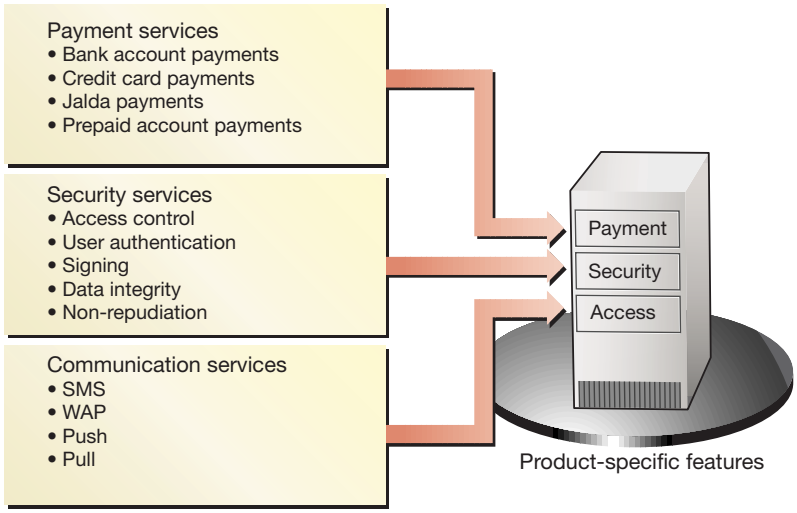


Figure 6
Mobile e-Pay end-user services and functionality.

e-commerce is used to aid them in complementing their range of services or in competing with other companies. Operators and service providers strive to position themselves in the market through differentiation from competitors, which enables them to rise higher in the chain of value-added services.

Benefits for ISPs and IPPs

First and foremost, mobile e-commerce can expand the overall volume of transactions for ISPs and IPPs. More transactions boost traffic and thus revenues. IPPs will reach the existing customer bases of ISPs, but they will also have access to completely new segments, such as end-users who use their mobile phones frequently. As they reach more users, the number of transactions will grow, enabling them to pay off investments faster, decreasing the cost per transaction.

Benefits for service and content providers

Service and content providers can offer services to new markets via this new distribution channel. Every person who has access to a mobile network is a potential customer, giving service providers virtually global reach. Electronic requests for new services allow customers to access them immediately, which means new revenue flows start immediately. Yet costs are reduced because transactions are executed electronically rather than manually. Mobile e-commerce solutions enable service providers to personalize differentiated services for narrower customer segments, such as young people and persons with financial clout.

In addition, service providers that deploy mobile e-commerce can gain direct access to new customers by partnering with major institutions, such as credit card issuers. They can boost their own customers' loyalty by offering the new mobile access method. What is more, they can take advantage of advertising via paging notices, which stimulates impulse purchases.

Retailers and banks are likely to use their massive brand and distribution strength to market mobile e-commerce terminals to high-value customers. Retailers will collaborate with banks and operators to offer marketable information services that make personalized content available via handsets and allow payments to be made electronically. The race is on to establish partnerships with

banks, travel agencies and other leading businesses that intend to use the mobile phone as a retail outlet.

Mobile e-Pay

Ericsson's solution, Mobile e-Pay, delivers mobile e-commerce services. As shown in Figure 6, the solution includes features for accessing the mobile network and the Internet (via WAP or SMS communication) as well as other functionality not directly related to security and payments. The security features provide authentication, encryption, digital signing and non-repudiation of transaction data. Payment features use direct links to manage accounts in financial institutions and those dedicated to mobile e-commerce.

Mobile e-Pay is offered in packages for the operator and the enterprise market segments. Each package provides a set of features for building flexible solutions for deploying new services. Mobile e-Pay is a scalable and modular solution, ready for rapid launch of mass-market services and prepared for the evolution of terminal and network technologies.

Mobile e-Pay's features for mobile financial transactions include security, payment, and mobile access functionality. These features are packaged for different market segments (Figure 7):

- The Mobile e-Pay Operator/ISP package targets mobile operators or mobile ISPs.
- The Mobile e-Pay Enterprise package targets service providers who want to offer secure transactions through multiple networks.

Mobile e-Pay is implemented as a set of functions on standard server platforms located in the e-commerce environment. For the mobile network, Mobile e-Pay interfaces with a mobile operator's own IP network, which gives it access to a WAP gateway and, optionally, SMS access nodes.

For the fixed network, Mobile e-Pay interfaces with content providers' WAP/Web applications. It can also interface with external financial institutions, giving access to credit card payments, and with certification authorities (CA) for integration into the public key infrastructure (PKI). The solution also supports connections with mobile financial institutions, provided an operator wants to offer dedicated financial accounts. In the Mobile e-Pay Enterprise package, the content provider and the financial institution might be the same service provider, typically a bank offering mobile banking.

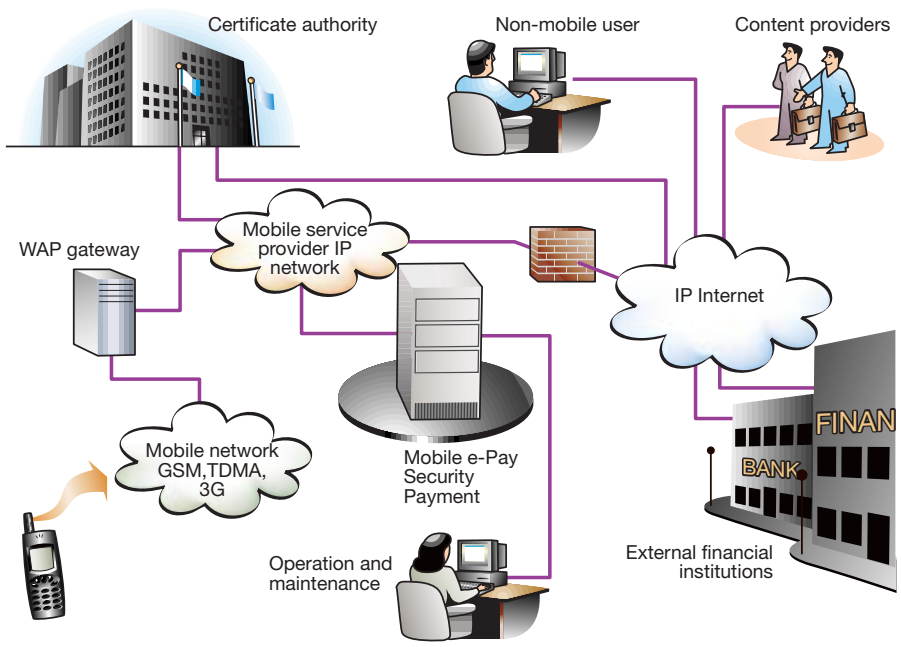


Figure 7
Mobile e-Pay environment in a generic network.

When deployed by a mobile operator, Mobile e-Pay is located on the operator's premises behind the firewall. When deployed by an enterprise, Mobile e-Pay is typically located inside the enterprise's IP network.

Mobile e-Pay's basic functionality supports financial transactions over the mobile phone and basic interfaces to payment or back-end systems (customization services are optional). The basic package also provides functions for converting algorithms to support security requirements; functions for converting fixed network protocols to adapt to mobile terminals (to support mobile network bearers); and operation, administration and maintenance (OA&M) functions, including transaction logging. Optional features provide payment solutions and browsing on mobile terminals.

Technical description

Mobile e-Pay includes access, payment, and security modules that form the core of the mobile e-commerce solution.

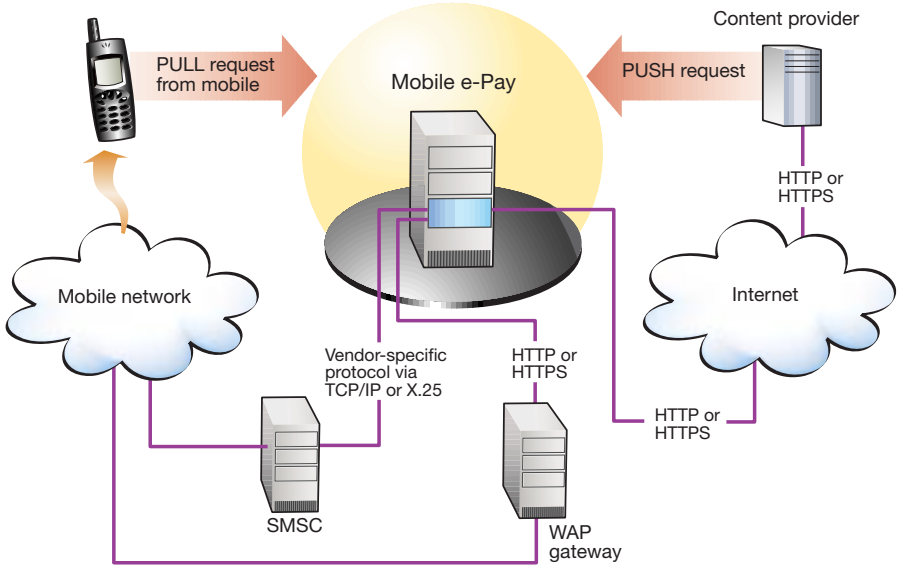


Figure 8
Access features with push-and-pull services.

Access features

Pull requests

When used for browsing, the mobile terminal communicates with content providers via a gateway—for example, a WAP gateway. A pull request occurs when the content provider directs a request (authentication or sign operation) from the mobile terminal to Mobile e-Pay (Figure 8). Mobile e-Pay processes the request and returns the results to the content provider, either directly or via a mobile-terminal redirect. Mobile e-Pay does not support pull requests using SMS and the SMS center (SMSC).

Push requests

Push requests are initiated from devices other than mobile terminals (for instance, a PC). Push requests are made to Mobile e-Pay through an interface to the content provider—in the example shown in Figure 8, this is done using the hypertext transfer protocol (HTTP). Until WAP-based push requests become available, push requests are handled using the SMSC. A push request is sent to an SMS gateway, which forwards the request to the SMSC using a vendor-specific SMSC communication protocol.

Mobile network

A WAP gateway or SMSC provides access to Mobile e-Pay (Figure 8). Mobile e-Pay currently supports WAP 1.1 and provides an HTTP interface to the WAP gateway, which should be able to provide an end-user ID. If necessary, an SSL connection to the WAP gateway can also be supported.

Internet

Content providers can access Mobile e-Pay using HTTP from an intranet or Internet connection. The interface to the content provider supports payment, authentication, digital signatures, and receipt handling. It also permits an SSL connection to be established. Mobile e-Pay might request the SSL connection during a pull request; similarly, the content provider might request the SSL connection during a push request.

Receipt handling

Depending on the application, a content provider might provide receipts (scripts available for end-users). This solution might not be acceptable, however, since end-users sometimes prefer to access receipts locally from their devices. Since WAP does not currently support persistent storage, Mobile e-Pay provides an "Info" interface that can be used to send receipts as short messages to end-user devices.

Security

Security is a key issue for mobile e-commerce, and application security systems are

being included in Ericsson's mobile e-commerce solutions. Designed primarily for financial services, such as banking and trading, Ericsson's security systems enable the completion of high-security transactions from a mobile phone. These transactions can include account balance inquiries, the transfer of money between accounts, billing services, and stock trading.

End-to-end security in the system means that the user's personal identification number (PIN), which is used to authenticate the generation of a digital signature, offers the necessary authentication and data integrity required to verify banking transactions. Each authentication is unique and does not rely on intermediary network functionality. The system also supports established techniques for data integrity and encryption, including wireless public key infrastructure (WPKI). The system can thus be integrated into existing IT infrastructure and security features.

WPKI, which consists of protocol extensions and software and hardware additions to terminals and networks that expand traditional PKI to wireless networks, is intended to enable the implementation of scalable security solutions that are independent of the application, network, and supplier.

PKI is an application-independent security infrastructure that is based on public key cryptography services for data integrity, confidentiality, authentication and non-repudiation. Using applied cryptography, PKIs govern the distribution and management of cryptographic keys and digital certificates that allow users to take advantage of several fundamental features.

- Confidentiality of information ensures that user communications are safe and can solely be read by the intended recipient. Message encryption using digital certificates guarantees confidentiality.
- Integrity of data guarantees that message contents are not altered during transmission between the originator and the recipient. PKIs provide digital signatures to ensure the integrity of all transmitted information.
- User authentication enables systems and applications to verify that users are who they claim to be and that they have been authorized to access resources. PKIs use digital signatures and user certificates to guarantee the authentication of all end entities and system resources.
- Non-repudiation prevents users of the PKI from falsely denying that they have participated in a transaction or sent a message to another user or resource. With a legitimate digital signature in hand and a legitimate digital certificate to accompany it, the chances of a message being forged or originating elsewhere are next to nil.

Security features and optional packages

Mobile e-Pay offers flexible packages of security features suitable for high- and low-value transactions.

- Two-zone (PIN) security. SSL is used to verify the identity of the parties and to encrypt the connection from the Mobile e-Pay node to the connected Internet node. In GSM, native network security is used for authenticating end-users. This scheme is enhanced with user pass-code schemes, which require end-users to know and input a pass code (a specific e-commerce PIN) to approve transactions.
- Two-zone PKI security. Using a PKI/RSA digital signature, Mobile e-Pay signs a contract after having presented it to the end-user. The digital signature is triggered when the end-user enters a static pass code to confirm a purchase. This feature, which does not require SIM application toolkit (SAT) support, can be used to receive and sign contracts from
  - WAP 1.1 terminals; or
  - plain SMS.
- End-to-end triple digital encryption standard (3DES) SAT security. End-users can authorize digital contracts with SAT-enabled phones. On a combined WAP 1.1/SAT phone, this means that message authentication code (MAC) authentication can be used to verify that the end-user approves the transaction. The 3DES key is stored in the SAT application. Any SAT phone—including non-WAP phones—can be used for push payments that are initiated from another terminal.
- End-to-end WPKI SAT security. The end-user can sign a digital contract using a SAT-enabled phone. RSA asymmetrical keys are supported. The private key is stored in the SIM, which enables the use of true end-to-end RSA keys with non-repudiation. Any SAT phone—including non-WAP phones—can be used for push payments that are initiated from another terminal.

For end-to-end SAT security schemes, the SAT applications are also protected by a personal PIN on the SIM. This protects end-users against misuse by persons who find or steal an authenticated GSM phone.

Authentication

To verify that end-users are who they claim to be, content providers must authenticate them. The results of an authentication operation are either *success* (that is, the user is who he claims to be) or *invalid* (a fraudulent attempt has been made).

PIN security

PIN security is the simplest authentication method. The end-user is presented with the contract and asked to input a secret PIN, which is returned to Mobile e-Pay. The application then authenticates the end-user by verifying the mobile station (terminal) integrated services digital number (MSISDN).

Digital signatures

Digital signatures are used to sign text or contracts, so that content providers can verify a user and ensure that a third party has not tampered with the contract. The results of a sign request are the text and a digital signature.

Security zones

Mobile e-Pay can provide end-to-end security or two-zone security. End-to-end security makes use of a SAT application which generates a digital signature on the mobile terminal that can be passed to content providers.

Two-zone security is defined as follows: Zone 1 comprises communication between the mobile terminal and Mobile e-Pay; Zone 2 comprises communication between Mobile e-Pay and the content provider. Mobile e-Pay verifies the end-user using PIN security. A combination of the phone number and a PIN are used to decrypt a private key and determine which security algorithm is to be executed. Mobile e-Pay can thus digitally sign contracts in proxy. The contract and signature are then delivered to the content provider. Two-zone security requires that the Mobile e-Pay system must reside in a trusted and secure environment (Figure 9). Mobile e-Pay might also add a certificate to the contract.

Confidentiality

In this context, we use the term confidentiality to mean that if a packet is intercepted it cannot be easily read. Mobile e-Pay can communicate with content providers using SSL, which provides Zone 2 confidentiality. However, since wireless transport layer security (WTLS) terminates an end-to-end solution in a WAP gateway, Zone 1 confidentiality is dependent on the mobile network.

Security methods

Mobile e-Pay incorporates the MAC, DES, MD5, SHA-1, and PKCS security methods.

MAC

A message authentication code is generated when a hash value of the contract is generated using a digest algorithm. The hash value is then encrypted with a symmetric algorithm and key. Some SIM manufactures support MAC generation. Mobile e-Pay currently supports MAC generation using the DES and 3DES symmetric algorithms. The key-hashing MAC (HMAC), which is a MAC mechanism based on cryptographic hash functions, can be used with any iterative cryptographic hash function in combination with a secret shared key. Mobile e-Pay supports message digest (MD5) and the secure hash algorithm (SHA-1). MAC generation algorithms can be implemented as a SIM application. Which of these algorithms is used, however, varies according to SIM manufacturer.

DES

The data encryption standard (DES) describes a block cipher data encryption algorithm (DEA) that encrypts data in 64-bit blocks using a 56-bit key that is shared by the communicating parties. Simply put, a 64-bit block of plain text goes in one end of the algorithm and a 64-bit block of ciphertext comes out the other end. DES is a symmetric algorithm; that is, the same algorithm and key are used for encryption and decryption. 3DES entails encrypting the data three times using DES. Mobile e-Pay supports triple DES.

MD5

MD5 is a message digest algorithm that takes a message of arbitrary length and produces a 128-bit fingerprint or message digest of the input. The MD5 algorithm is intended for digital signature applications, where a large file must be compressed securely before it is encrypted with a private (secret) key under a public-key cryptosystem, such as RSA.

SHA-1

The secure hash algorithm is used for computing a condensed representation of a message or data file. When a message of any

length less than 264 bits is input, the SHA-1 produces a 160-bit output called a message digest. This can be fed to the digital signature algorithm, which generates or verifies the signature for the message. The same hash algorithm must be used to create and verify a digital signature.

PKCS

The public key cryptographic standard no. 1 (PKCS#1) is the standard method for encrypting data using the Rivest-Shamir-Adleman (RSA) public-key cryptosystem. For digital signatures, the content to be signed is reduced to a message digest with a message-digest algorithm (such as MD5). An octet string (which contains the message digest) is then encrypted with the RSA private key of the signer of the content. The content and the encrypted message digest are represented together according to the syntax in PKCS#7 to yield a digital signature. Mobile e-Pay returns PKCS#7 format signatures for the MD5 and SHA-1 security methods.

Payment features

Mobile e-Pay payment features enable providers to offer a complete payment solution which gives end-users a new electronic wallet that is accessible via the mobile phone. Thus, mobile users can use their mobile phones as a device for paying for goods or services.

Basic payment features

Ericsson has developed a standard communication interface to the payment server. Operators can use this interface to integrate Mobile e-Pay into any suitable payment server solution—for example, if they do not purchase the payment servers offered with Mobile e-Pay.

Jalda payment features

Jalda is a multipurpose payment method that supports convenient, fast and secure financial transactions on the Internet. It is open and flexible and can handle transactions of any amount—from fractions of a cent to huge sums—without requiring the transfer of credit card numbers or electronic currencies. Jalda is a session-based Internet payment method that enables payment by the second, item, quantity, mouse click, search, character, page, or practically any other parameter. Jalda consists of two parts:

- an application program interface (API)—the Jalda API; and
- a payment server that administers user data and keeps track of transactions.

The Jalda API can be embedded into virtually any application, which paves the way for content and service providers to sell goods and services on the Internet and to reach end-users on wireless networks. All transactions between the end-user and the content or service provider are managed by a trusted third party—an Internet payment provider—who owns and operates the payment server.

Mobile e-Pay can connect to Internet e-commerce applications using the Jalda API. Doing so extends the Jalda payment standard toward mobile end-users. In a configuration in which the payment system is on the Internet side, mobile users can thus use their mobile phones to sign digital contracts.

Payment features including payment server functionality

A payment server, which is offered together with the mobile pay features, serves the interface to external financial institutions, such as credit card companies. It also logs all financial transactions.

Credit card payment

When end-users subscribe to Mobile e-Pay, they can register one or more credit cards in the Mobile e-Pay system. They can then use these cards to pay content providers for goods and services. Payment is made online via the card issuer, which is to say that users can leave their cards at home and instead use

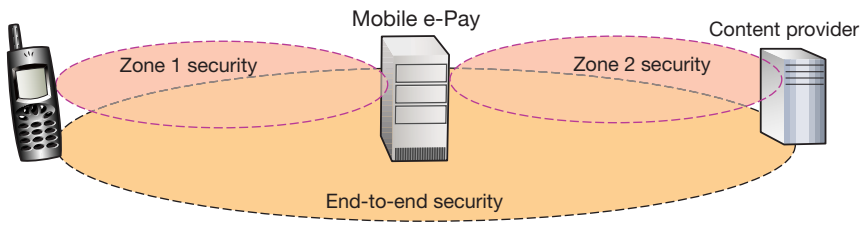


Figure 9
Two-zone security or end-to-end security alternatives.

BOX C, MARKET HARMONIZATION

On Tuesday, April 11, 2000, Ericsson, Motorola and Nokia announced that they have teamed up to create a common framework for mobile e-commerce. The main objective of this joint industry effort is to ensure complete market harmonization in terms of how certificates, keys, processes and services are implemented in mobile phones and offered to end-users. The framework for how mobile transactions are to be handled and implemented will be drafted and distributed for comment from related players in the industry (operators, service providers, bankers, credit card companies, retailers, and so on). The framework will be based on the wireless application protocol (WAP), WIM/WTLS, WPKI and Bluetooth.

the phone as a payment device. Support is offered for several major credit cards, including VISA, MasterCard, American Express and Diners Club.

Mobile e-Pay prepaid account

A dedicated e-commerce prepaid account can be connected to the mobile e-commerce service. The prepaid account, which is administered and issued by the Mobile e-Pay operator, can be used to pay content providers for goods and services. Mobile users can check account balances from their phones. The accounts can be filled manually by the Mobile e-Pay operator, or users can fill them using credit cards in combination with the *credit card payment* or the *bank account /debit card payment* features.

Bank account/debit card payment

The payment server can implement market-dependent interfaces to partnering banks or national banking networks. The implementation of market-specific banking interfaces is a common practice with payment server deliveries. Bank or debit card payment is not part of the standard Mobile e-Pay offering. To the end-user, the procedure is the same as for credit card payments.

Content provider API (software library) for payments

An application program interface and an IP connection are all that content providers need to connect to Mobile e-Pay payment functions which are connected to financial institutions. To use Jalda payments, a separate Jalda API is also needed.

Conclusion

Although the global digital economy is still in its infancy, it will grow to support a huge and complex market. Service providers who have the tools that help consumers experience this new market as easy-to-understand, user-friendly and convenient will be hands-down winners. In fact, we might define the true value of mobile e-commerce as the ability to make specially tailored services directly available to the consumer via a familiar, portable device.

For mobile operators and content and service providers, mobile e-commerce represents a new way of adding value and of differentiating the services they offer, as well as of expanding their markets and building customer loyalty. It is quite simply an entirely new sales and promotion channel. Unlike brick-and-mortar retail outlets, mobile e-commerce can be thoroughly tailored to a consumer's individual needs and tastes. And it is available to that consumer anywhere, anytime. In short, mobile e-commerce is all about consumer empowerment.

The right combination of mobile systems, Internet, payment, and security technologies now exists to make mobile e-commerce a commercial reality. Ericsson's Mobile e-Pay solutions enable operators and service providers to generate new classes of service based on each user's geographical location and personal profile. As the world wakes up to the huge potential of mobile e-commerce, mobile operators and service providers will have the unique opportunity to establish a lead in the market.