ATM in your Pocket - The **Mobile** Phone as a **Payment Device**

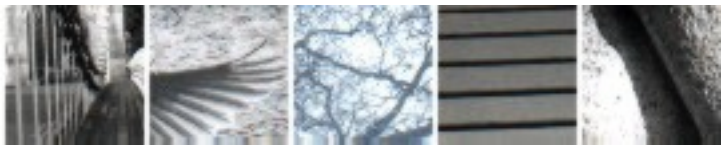
When you write a cheque or use your credit card to pay for a service or desirable object, money is not exchanged but information is, eventually resulting in an electronic funds transfer. The information required to perform the transaction is simple, but the cheque, credit card slip or electronic till is only a carrier of the data, and dependent upon other processes to carry it to its final destination.

The personal terminal, which will, amongst other things, provide you with mobile telephony services, can generate and transmit all the data necessary for a financial transaction to take place. In fact like a debit card, the data transmitted from the terminal can cause an immediate transfer of funds from one bank account to another, resulting in a "cash like" transaction, hence the terminal becomes your personal ATM.

Data vs. Cash

The preferred method of payment for goods and services today is the credit or debit card. They save us having to carry large quantities of cash around, although there is still a need for small sums of money for items that are so cheap that they don't justify the transaction costs. So we have a variety of plastic cards in our wallets offering a choice of payment methods (plus some cash in our pockets).

When cash is used in a financial transaction it is straightforward; a sum of money is handed over and a service is performed or goods are received. Immediately after the transaction both parties have their required result. On the other hand, using a plastic card to pay for something is a more complicated affair. Data is transferred between two computers (one of which is the EFPOS or Electronic Funds Point Of Sale terminal, and the other is a bank computer), but no money changes hands. Eventually of course records are exchanged between bank computers and one account is credited while the other is debited, but this may not occur for several days (up to a month with credit cards). In addition there are costs imposed by banks for providing



support for these plastic card transactions, which either reduce the profits of the vendor, or increase the costs for the purchaser.

It is worth considering for a moment what actually happens when a cheque or plastic card is used as a payment (i.e. when cash doesn't change hands). Instead of cash, information is exchanged between the two parties, and trust between the two parties (which would be very tenuous if it were unsupported) is backed up by a promise of payment from the bank concerned. The information received by the vendor is passed on to his bank which uses it to extract the electronic representation of money from the purchaser's account, and place it in the vendor's account. Clearly somewhere the information exchanged must include permission to access the purchaser's account.

There is an underlying theme here, even when payment is made by paper cheque, the result is a transfer of data from one bank to another, through the interconnection of their computers. What happened to money? Money of course only enters the equation when real cash is required for those transactions unsuited to electronic payment, all the rest is just data.

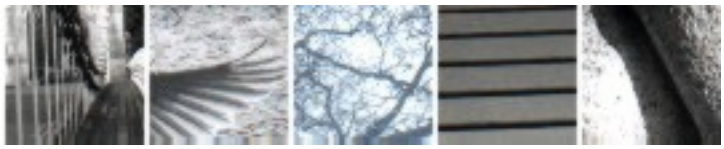
There is now considerable interest in Internet access and access to other data services from cellular phones and PDAs as well as Internet purchases. So if an advanced wireless phone/PDA (i.e. personal terminal) contained suitable functionality what would be the advantages or disadvantages of including such a device in the transaction process?

The Background of the Personal Terminal

Impact of digitisation of cellular networks
During the last decade of the twentieth century, cellular phones changed from analogue to digital. Speech was digitised in the handset instead of, as previously, at the radio base station (the point in the network to which the handset connects). There were other changes associated with this "digitisation", some of which we will touch on later, however digitisation itself led to one fundamental difference - if data was to be transmitted, no modem would be required for data communications.

With digitisation came the possibility of easily connecting an external, portable, computer. The data rate available on these second generation (2G) (analogue systems such as TACS were 1G or first generation) cellular systems at 9.6kbps, was better than anything that had been previously available in the mobile environment. In fact it was not much different from the speed of dial connections that could be realised on a fixed telephone. These were exciting times, and many assumed that data services would soon compete with voice for traffic across the mobile networks.

Advances in personal computing
At about the same time, there was an increase in the number of computers purchased for home use. At first there was little need for a modem, as there was little other than direct computer to computer file transfers that could use it. However, when the Internet and e-mail started to be adopted by people working away from the office, the speed of modems dramatically increased. Very soon it was quite normal to buy a PC with a 28.8kbps modem built in and by the end of the '90s it was possible to have a 56kbps modem, ISDN at 64 or 128kbps and much more. Unfortunately, digital cellular phones were still stuck at 9.6kbps. The advances in modem technology had not helped the wireless environment and data services did not expand to compete with speech.



Organisers and PDA
In parallel with these developments a new computing device became available. Initially simple electronic diaries that could hold a few addresses and telephone numbers, these devices quickly became fully programmable such as the Psion Organiser. These "handheld computers" lacked the power of full desktop PCs, but offered almost pocket size computing, with full diary, address and phone book functionality as well as the possibility of third party software for other functions.

These devices changed from being organisers, a sort of electronic FiloFax, to being Personal Data Assistants (PDAs) and the only function lacking in them was an ability to talk to other computers to share data. Initially this connection was included by wire directly to a host computer and then by InfraRed transmission (the first form of wireless computer interconnection). This allowed the sharing of address book data, downloading of data such as product prices from the corporate database, and finally the up and downloading of e-mails which was becoming a greater and greater necessity for everyone whose work revolved around a computer.

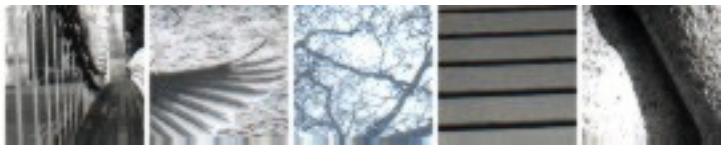
The PDA today is a sophisticated device with a colour display, capable of displaying graphics in just the same way as a PC screen. In addition touch screens allow interactive use of icons without the need for a mouse, and software that can "read" handwriting does away (at least partially) with the need for a keyboard. Indeed many PDAs do not have a keyboard at all, putting a "virtual" keyboard on the display when one is needed.

There is an obvious requirement for a PDA that can transmit and receive its data over great distances so that the user can be anywhere and still "synchronise" with data in his office. Ideally such a device should double as a cellular phone using the same wireless infrastructure. This requirement has been partially met in devices such as the Nokia 9000 Communicator, but it is still hampered by the low data rate of 9.6kbps. While this is just about enough to allow updating of address books and even sending and receiving of short e-mails, for anything else it is just too slow. The PDA functionality is now sufficiently advanced to be used to access the Internet and its wealth of information, but existing mobile data rates would make the time to download a conventional web page just too long.

New communications protocols
A protocol has been developed to partially overcome this speed shortcoming of mobile handsets. WML (Wireless Mark-up Language) is used at the heart of the Wireless Access Protocol (WAP). This protocol minimises the amount of data downloaded to the handset to the bare essentials, and to what can be managed by the terminal display. With a suitable "micro-browser" installed in the handset it is possible to access web sites that have been WAP enabled and see the results directly on the handset. However reducing the information to overcome the handset's shortcomings is only a short-term answer. What's needed is a higher data rate delivered to the handset, which would justify the inclusion of full PDA functionality in the mobile handset, converting it into a full personal terminal.

New Technology Developments Towards The Personal ATM

Assuming that the personal terminal held the appropriate data, it could emulate any number of plastic cards. This would immediately do away with the need to carry a variety of cards, simply select the credit or debit function and one of the banks with which you have an account from a simple menu. Now what? It is not feasible to swipe a terminal through a shopkeeper's till so the "card" data has to be transferred by another method.



It is time to take a look at current technology developments to establish the ways in which this data might be best transferred, and to whom.

An imaginary multifunction smart card, including GSM SIM; credit, debit and cash card; and entry control functions.

The introduction of digital cellular systems also introduced the concept of the "smart" card. In a GSM[1] phone this is the SIM (Subscriber Identity Module), and although it is the same size and thickness as a credit card, it contains all the elements of a computer (central processor, stored program and memory). Smart cards are now being used in a variety of ways including holding of medical records, identity cards, entry and exit control mechanisms and some banks in Europe use them instead of magnetic stripe credit cards. Multi function cards are now becoming available and these will open the way for cellular phones to act as the intermediary between card functions and the outside world - wirelessly of course.

Second generation phones pointed the way towards data transmission and highlighted some difficulties. Enhancements to this technology are resulting in so-called 2.5G terminals that will carry data in a more efficient form (packet data) and faster (at least 28.8kbps, and quite feasibly 56kbps). This will in turn lead to a closer link between PDAs and mobile terminals, probably resulting in the first personal terminals. At this point there is the possibility of the terminal transmitting all the necessary data from the smart card for a financial transaction. But there's more. A new wireless technology is about to be unleashed called Bluetooth.

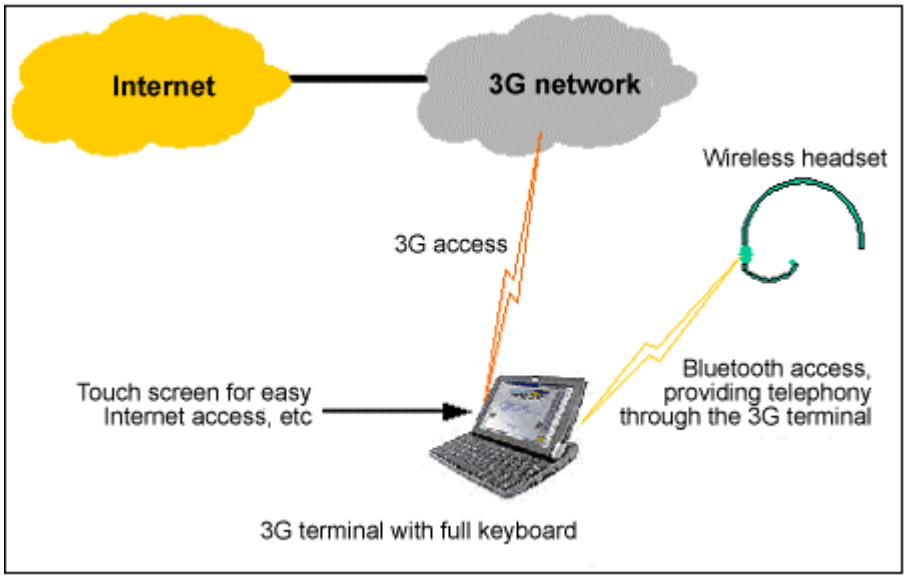
Bluetooth is a short range radio technology (~10 metres) that is self organising. That is to say it will establish links with other Bluetooth devices whenever they come into range. The data rate is more than compatible with 2.5G being up to 0.5Mbps. The intention is to build mobile handsets with Bluetooth included so that external devices, such as headsets and computers can be connected in a wireless fashion through the handset into the telecommunication networks. This makes the handset more of a communication gateway than a phone and if required it could be left in a briefcase even while in use.

Add to this the even further evolved mobile communication system UMTS (third generation or 3G) providing truly high speed data (theoretically up to 2Mbps though more likely to deliver up to 384kbps), and several communication transactions simultaneously, and there are several ways to conclude our electronic purchase.

Our terminal now carries the smart card with all our credit card type details. We select the type of transaction (credit, debit and which bank), and either directly transfer the data to the vendor's bank, or perhaps more realistically, the data can be wirelessly transferred (via Bluetooth) to the vendor's terminal, and from there, treated in the same way as a swiped card. The big difference would be that all data associated with the purchaser is contained on a single smart card, regardless of the type of transaction, and this data is never exposed to other people, reducing the possibility of fraud.

[1] GSM is used in this text to refer to 2nd generation cellular telephony systems, it could also refer to CDMA (US) where this is implemented with a SIM or similar device. UMTS is similarly used to refer to 3rd generation systems

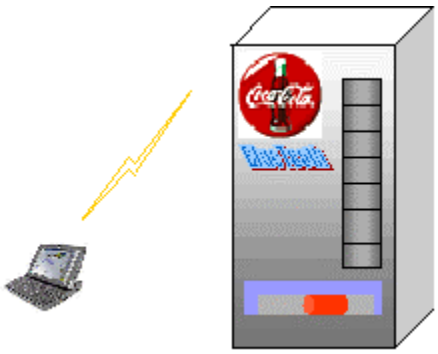
A wireless payment service similar to that described above called "Paybox" is offered by paybox.net AG GmbH. The service offers credit based services for which a small subscription fee and a 3% transaction fee is charged for each purchase.



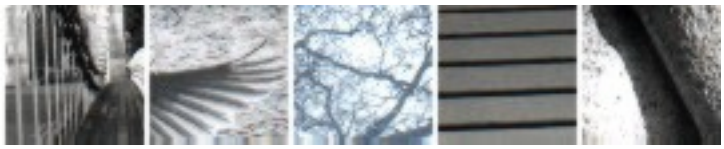
An example of a personal terminal with wireless headset for voice access and a touch screen for easy control of web browsers etc.

Certain transactions are simpler than those described above. Using a vending machine to purchase a soft drink for example usually requires a few coins, and if you're lucky, the machine will give change. Experiments have already demonstrated the viability of purchasing the drink by dialling the machine from a cellular phone and passing credit card details to it, resulting in a drink being dispensed. This unfortunately incurs the credit card transaction cost and is unlikely to very attractive. However the concept of this "proximity payment" is attractive, and with two modifications could become a very popular service.

- The use of Bluetooth would ensure that the purchaser didn't buy a drink unless he/she was near the machine (no accidentally buying a can of Coke in Canada, when you're in Sydney because you have entered the wrong phone number!).
- Electronic cash would eliminate transaction costs.



Electronic cash is a system on trial in several places around the world and allows the transfer of relatively small amounts of money between individuals as well as between banks and their customers. Cash equivalent is downloaded to a smart card (and this can be the smart card in our personal terminal of course) from a bank account. When this cash



is downloaded, the account is debited just as if an ATM had been used. The cash equivalent is held on the card until it is transferred to someone else's card through telephone, Internet or directly to the shopkeeper's till, again using Bluetooth. The transactions do not involve a third party at any time and hence incur no charges. Now buying a soft drink simply requires that the purchaser stands within 10 metres of the vending machine, selects the drink from a menu presented to him on his personal terminal, and gives permission for a small amount of cash to be transferred to the machine.

Pro-active Vending

The use of electronic cash cards and proximity payment provides a novel new method of marketing products. Imagine the case of the vending machine above equipped with BlueTooth and an ability to accept electronic cash. As you pass close to the vending machine, it detects your BlueTooth equipped terminal and alerts you to the produce it has for sale. It generates a menu on your terminal screen and offers you the "special" (because it has more of this than other drinks within its stock) at a 10% discount. As no real cash will be exchanged there is no problem with varying amounts of change. You accept the suggestion by touching your terminal's screen and you get a drink even though you hadn't been actively searching for one.

The possibilities for this kind of pro-active machine marketing are enormous and will include active advertising from billboards, and transmission of menus from restaurants etc. It is likely that users will want to limit the number of advertisements they receive and it will be necessary to include some filtering in the personal terminal.

Security

In any financial transaction, security must be the first concern of all involved. There are several areas of security that must be considered and any new system such as wireless payment must address all these issues.

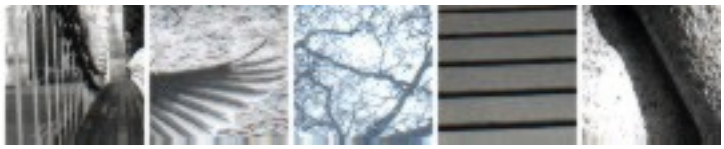
Data protection
Details of the purchaser that might be required for the transaction, must be held securely and not passed on to third parties without permission.

Fraudulent use of the purchaser's details
Cases of credit card numbers and expiry dates being fraudulently reused by people who have "acquired" these details (just by looking over someone's shoulder for example), are not unheard of.

Illegal wire tapping
Transactions that involve the use of telephones or mobiles are susceptible to unauthorised persons "extracting" relevant data and re-using it as described above.

Card loss
If a credit or debit card is lost, its ability to be used illegally can usually be stopped quickly.

Identity verification
It is important to ensure that the owner of a card is who he says he is. This is usually achieved through the use of a signature, but in mail order transactions and some other circumstances this is not possible.



The points listed above probably do not cover all the security issues, but they are all serious and it is worth considering how a personal terminal might address them.

In a GSM call, a great deal of information is passed between the network and the phone before a call can begin. Initially (when the phone is turned on) the network needs to verify that the user is a paid up customer. While it is not actually possible today to ensure that this is the case, the next best thing is to ensure that the identity module (SIM) represents a valid customer. The process of verifying the SIM is very secure and one of the results is that all subsequent communication between the handset and its base station is encrypted using a highly secure algorithm and a unique set of encryption keys. What this means to a financial transaction is that if the mobile network verifies the user as bona fide, then they probably are.

For a financial transaction (other than perhaps electronic cash) this would only be the first check, but the facilities exist for encrypting transactions ensuring there is no "eavesdropping".

An added feature here is the fact that the customer details are held centrally, and do not enter into the transaction at all. There is therefore no data protection issue.

By never handing a card to anybody else, the chances of re-use of the information are largely cancelled. Only machines are aware of the actual data, and it can always be transported, and held, in an encrypted form.

Card loss would probably involve terminal loss as well, and informing the operator of terminal and SIM loss would result in the SIM being "disconnected". This can be arranged to suspend all other activities on the smart card, thus securing the financial aspects from abuse.

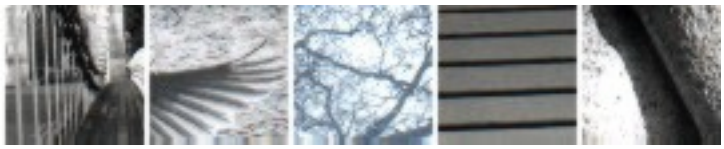
How long before it happens?

All the technology described here is available or about to be launched. Multi function smart cards, cash on a card, enhancements to GSM (GPRS has already been launched by some operators) and Bluetooth (available now, but a little while before enough devices have it built in). It is a question of integration rather than development and could happen sooner than you might think.

Finally

It is clear that the communication capability and inbuilt functionality of forthcoming personal terminals will make them an attractive alternative to a multitude of plastic cards. There will be improved and increased services (imagine paying your restaurant bill, at your seat without handing over a card, and in your own time!) an increased level of security and perhaps most important, a reassurance of increased control through retaining the financial data throughout a transaction.

The ATM in your pocket may not print your bank notes, but it will do everything your bank notes could, and considerably more.



This paper was first published on in September 2000 on www.virtualbanking2000.com - a virtual conference and exhibition about the current virtual banking world.

An Intercai Mondiale White Paper **Tel: (0) 1628 478 470**

Intercai Mondiale Ltd, Regatta House, High Street, Marlow, Bucks SL7 1AB, UK

www.intercai.co.uk