



White Paper

Issues To Consider Related To The Development Of Mobile Internet And Data Services Over Cellular Environments

Prepared by: Peter Benson
Senior Consultant
EMS-Global

Date: May 2000

TABLE OF CONTENTS

ABSTRACT	3
SUMMARY.....	3
THE SCENE:	3
ANOTHER PERSPECTIVE FROM INKTOMI:.....	5
APPLICATION DEVELOPMENT	6
THE LAST MILE	8
AUTHENTICATION MECHANISMS FOR E-COMMERCE	8
ENCRYPTION ISSUES	10
APPLIANCES, NETWORKS AND DEVICES.....	10
SECURITY ISSUES.....	12
REFERENCES:.....	14

Abstract

Over the next couple of years, expect an explosion in the growth of next generation wireless systems, with subsequent explosions in the growth of applications and services aimed directly at the mobile market.

This paper explores some of the issues from a high level, and identifies areas that need to be considered before organisations take the leap into the on-line mobile world.

Summary

The development of the mobile environment is in a fragile and formative state at present. This is where the industry is starting to identify potential opportunities for profit and revenue, but also where the technology is still relatively unproven and immature. A few **New Zealand** companies and service providers are starting to move towards high speed mobility as a key future direction for their development, but production systems at present are still relatively immature and primitive. This white paper identifies EMS-Global's perspective and vision on some of the areas of interest in the development of the mobile arena.

The Scene

From www.msn.com

“What's wireless broadband? And why it's so powerful?”

“ The truth is that wireless data transfer isn't particularly fast or reliable. It currently runs at just 9.6 kilobits to 14.4 kilobits per second -- a whole lot slower than the 56 kilobits per second speed of that modem hooked up to your PC at home that you complain is already too pokey. That's why the wireless companies are virtually giving the service away. Sprint PCS (Personal Communication Service, for example, will let you sign up for its wireless Internet service as a \$10 a month add-on to its regular PCS service.

“But you know what? The wireless industry also isn't spending anything significant to provide this toy. Nobody's upgrading their network to deliver stock quotes to a few thousand customers. If somebody buys a more expensive Internet phone instead of a basic model from [Motorola \(MOT\)](#) or [Nokia \(NOK\)](#), that's gravy. The \$10 a month is a little incremental revenue to pay for some of the marketing campaigns.

“Getting ready for the big rollout

“All that the wireless companies are doing right now is getting the market ready for the rollout of the next generation of wireless broadband technology -- or maybe it's more accurate to say technologies. In the time-honoured tradition of the wireless industry, these companies are backing two competing standards – CDMA (**Code Division Multiple Access**) and General Packet

Radio Service. (Each of these "standards" has major variants, such as AT&T's Cellular Digital Packet Data, which is related to General Packet Radio Service.) These should hit the U.S. market in mid-2000 (in the case of General Packet Radio Service) or mid-2001 in the case of CDMA. (AT&T is offering Cellular Digital Packet Data in the United States now.)

“Both CDMA and General Packet Radio Service offer really big increases in speed over the current 9.6 kilobits-per-second rate. According to Michael Murphy, editor of the California Technology Stock Letter, General Packet Radio Service promises 100 kilobits per second -- about 10 times faster than the current wireless standard. The new CDMA standard will be even faster at 128 kilobits per second. That's about twice as fast as the current 56-kilobit home PC modem.

“That speed probably isn't fast enough, however. You know how long it can take to load an Internet page at home. No one will stand around in the street waiting that long. So these new technologies play tricks to make the Internet faster. For example, Nokia and other companies backing the General Packet Radio Service standard are also pushing a technology called Wireless Access Protocol, or WAP. A WAP server -- and Nokia is currently giving these away -- automatically rewrites a Web page from the HTML language into the simpler WAP language to speed up delivery.

“Wireless data speeds will continue to increase with time, but the development path for this technology is pretty clear. The next generation will be faster than the standard PC modem operating over standard copper wires, and about as fast as ISDN. (Remember that technology?) It will still lag the 640 kilobit speed of DSL, but even at 100 to 128 kilobits, wireless is in the game.

“Four ways that the game will change

1. “First, it accelerates the rate at which U.S. consumers, following in the wake of their European counterparts, go off the wire. More and more wireless users around the world are opting for wireless as their only phones. But a consumer who went off the wire for voice, still had to stay on some wire (or cable) for data and the Internet. Not any more.
2. “Second, wireless broadband will make the market for Internet appliances explode. Any appliance with a radio frequency chip set and a wireless modem can hook up to the Internet. Nothing has to hook up to a phone jack, which means you can put an appliance anywhere in a house, a car, or in a bag, backpack or pocket.

3. "Third, wireless broadband will heat up the struggling market for home networks. Internet appliances all need to be co-ordinated -- can't have personal calendars or stock portfolios out of sync. But the current solutions for updating all the devices an individual uses are awkward. Infrared communication requires a clear line of sight. Physical docking requires, well, physical docking of each device. But the wireless home network would consist of just a hub, connected to the Internet, that co-ordinates and swaps data between all the devices you own using radio frequencies and software. The consumer at home would have all the advantages of a workplace Ethernet -- including Ethernet speed -- without the wires. Want to see what that device would look like? Check out Apple's AirPort wireless base station.

4. "The consumer market for wireless broadband will give a huge push to the business market. As wireless devices provide central access for data, the logic of building wireless corporate networks increases. At the least, workers who use wireless devices will want to be able to access the corporate network, which may, in part, go wireless even inside the office. And, going even further, some corporations will opt for going wireless with their whole network for data access and transmission."

Another perspective from Inktomi:

"Last week Inktomi announced it would bring its Internet infrastructure software to wireless with offerings to carriers, portals and enterprises. Inktomi also announced an investment in AirFlash Inc. for mobile phone Internet services plus alliances with Cap Gemini, Portal Software, Hewlett-Packard Co., Sun Microsystems Inc., Spyglass Inc. and wireless application service provider GWcom Inc. for what the company called an end-to-end solution.

"Wireless analyst Jane Zweig of Herschel Shosteck Associates Ltd. says Inktomi's announcement was "impressive in terms of the partnerships," but it is only the latest in a series of partnership announcements that Internet companies are making in the wireless business. Only the future will determine if these partnerships are different enough to set themselves apart in any way, Zweig says.

"Everyone is competing to deliver on the generic message of 'any content, anywhere, any device.' It's like a mantra," she says.

"Inktomi's president, David Peterschmidt, says the company will

invest significantly in the wireless arena because it was to be the "de facto provider of core technology for the wireless Internet." Julie Keslik, an Inktomi spokeswoman, says carriers have told the company they want an end-to-end solution that allows them to establish a wireless Internet portal quickly and efficiently.

- **March 20, 2000 issue of *Wireless Week***

Application Development

So what do we think ?

Application development will increasingly use the Wireless Access Protocol (WAP) for the communications, with browsers capable of using and displaying languages such as Wireless Markup Language (WML), and HDML. Secure communication and delivery of information will increasingly use Transport Layer Security (TLS), specifically developed for Wireless communication. Increasing development will occur in new encryption algorithms and schema, specifically tailored for the lower speed delivery mechanisms. Current development focus is increasingly on Elliptic Curve Cryptography (ECC), which has the potential for reduction in the computing power needed for secure communications.

Delivery of content to mobile appliances is expected to include all current forms of content used across the Internet and other delivery mechanisms, including video, audio, transaction based data, and potentially proprietary data. One of the leaders in the field is Phone.com, with their UP.Link product set. Portals will be developed (are being developed now), that translate HTML or web based systems into WML for use in wireless applications.

A number of proprietary systems will be developed over the first few years, which will slowly be absorbed into more mainstream development. For some time, it is expected that there will be a fight for the browser market, for both the browser and software installed in the mobile device.

Already there have been developments in this field, with groups like the Commonwealth Bank of Australia having developed custom applications for on-line mobile phone banking. This uses a proprietary application installed on the SIM card in GSM based phones. In the example of Nokia based GSM phones, this provides additional menu options in the phone display system, for direct banking.

Application development is expected to accelerate over the next 1-2years, and tapering off by approximately 2004 – 2005. The expectation is that this will be the Internet delivery mechanism of choice, and is likely to take over broadband Internet connections for the average user. Business to Business communication is still expected to operate over fixed services, and will often extensively

use proprietary IP based delivery networks.

Initial application development is expected to take the form of the following:

- Mobile portals, which translate the current Internet capability into something useable for Mobile users with limited displays and bandwidth. High use is expected of WAP translation software. Nokia are currently giving away their version of the translation server to encourage the development in this space.
 - Specific applications will be developed for use with mobile users, for example mobile banking, multi media, broadcast, messaging, subscription services, tourism (high expectations).
 - Specific mobile targeted applications, which will take direct advantage of the mobility aspect. This may include linkage to peripheral devices such as the car, GPS systems, etc.
-

The last mile

The Mobility delivery system is a combination of Internet appliance, and conventional Internet infrastructure networks with wireless as the last arm of the delivery mechanism. In reality the mechanism for delivery is inconsequential, apart from the issues of bandwidth, and the nature of being broadcast over an inherently insecure medium for the last mile (i.e. radio). As the Internet is generally considered a public medium, the issue is primarily that of privacy concerns driving the technology. In general, standard data protection mechanisms will need to be in place, in line with any other public medium.

Over time, there is a high expectation that the cost of the delivery mechanism, regardless of whether this is broadband DSL, or CDMA, will tend to transition towards zero. The push will be strongly towards the service offering as the revenue opportunity, with the delivery mechanism, either copper or radio, will be of effectively zero cost. Already in the dial-up Internet market, we are seeing “free” offerings of PC’s and Internet connections, with the revenue opportunities coming from the advertising and content provision. There is no reason not to believe that CDMA delivery mechanisms will not go the same way.

The key to the opportunities offered are that the end appliance can be located anywhere, without the need for the provisioning of a physical infrastructure to provide the connection. The device or appliance can be made to operate even in motion, which opens up huge opportunities for the development of applications that are designed specifically to take advantage of geographical based processes.

Authentication mechanisms for e-Commerce

One of the key *issues* facing the cellular industry at present is fraud through cloning, and misuse through theft. One of the key *problems* facing Internet e-Commerce, is the issue of authentication, and non-repudiation. In the Internet world, identity trust is key to success in completing transactions in a way that satisfies the need for determining that people are who they say they are, and that they have the authorisation to make the transactions. The obvious areas in which this becomes an issue is in credit card transactions, where proof of authentication is in (generally) having both the card details, and some form of corroborating information, such as name. When the card information is disclosed to unauthorised persons, the card can be, and has been, used with impunity. While there are generally limits as to the user’s liability, this does not preclude the fact that the users identify has been stolen, even for a short period of time. This issue of identity theft will be discussed further.

In the case of bank transactions, or negotiating encrypted connections, higher levels of security are required to ensure that identity and authentication is completed with a reasonable degree

of security, and that there is a reasonable degree of confidence that the transaction is valid. In the case of Internet secure connections, using SSL for example, the transaction is negotiated using digital certificates to establish the trust relationship.

In mobile systems, the use of digital certificates will become more valid, and of more practical use, as the user becomes intricately bound to the device that contains the digital certificate. In the past, there have been attempts to provide mobile certificates for users based on smart card technology, however the use of mobile appliances that contain the certificates provides much greater scope for secure transaction developments.

The big issue however is that the user's identity now becomes bound to the device within which the certificate is kept, i.e. the physical phone or mobile device. Loss or theft of the device causes immediate issues around the notion of identify theft, and potential issues around proof of identity to other parties without the device. Processes and mechanisms will be required, both in business and in the technology, to keep the privacy and integrity of the individual's identity intact. This will be one of the big challenges in the next 1 – 2 years. There have been prototypal developments of mobile devices with biometric capability, i.e. thumb print readers, however these are not yet released in any large way into the commercial market.

As an indicator of industry trends, twenty-eight security companies earlier this year formed a global initiative called Radicchio to promote Public Key Infrastructure as a technology for secure wireless transactions. Among the companies are 724 Solutions Inc., Baltimore Technologies Inc., CYLINK Corp., Certicom Corp., Entrust Technologies Inc., Ericsson, Gray Cell Inc., iD2 Technologies Inc., Lucent, MasterCard International Inc., Saraïde Ltd., Synamic Ltd., VeriSign Inc., Virgin Mobile Plc, Visa International Inc. and Vodafone AirTouch plc.

Encryption issues

Encryption is the cornerstone mechanism of providing for confidentiality, integrity, and non-repudiation within the business and Internet space. In the Internet world, this is generally performed using SSL for secure communication, and digital certificates / secure messaging / proprietary encryption mechanism for file and data security.

In the wireless space, there could be the potential for complacency in an expectation that the wireless coding methodology provides the encryption and hence the security required. In reality, most of the current coding systems are based around the delivery design capability, and are not specifically designed to provide end-to-end security. In regards to data communication and Internet communication, remember that the wireless delivery is only the “last mile” of the communications path. Already there is anecdotal advice that the GSM protocol has been broken, however we have yet to see any practical example of this.

New encryption standards are expected to be developed for wireless communication, to take into consideration the bandwidth restriction, and the likely limited computing power of the handsets / devices. In the case of current communication, most of the current public key cryptography is based around the RSA designed schema, which require a reasonable degree of computing capability for processing the encryption and decryption. Over the next year, expect to see a number of “appliance” specific standard schema coming out, that are capable of being embedded into low-end appliances. Elliptic Curve Cryptography (ECC) is expected to have a huge impact on the industry over the next couple of years.

Appliances, Networks and Devices

There will be a surge of development into wireless “devices”, although voice will have a premium on the use of the mobile systems for the next year or so. Over time, there will be increased use of “plug in and turn on” devices, for which wireless systems lend themselves perfectly. Areas in which we expect developments to come include:

- Intelligent kiosks, mobile devices, wireless LAN connections
- Lap tops and PDA’s will have radio modems as optional peripherals for direct connection
- Remote devices that have reasonable data transferal requirements will leverage off mobile technology to reduce data transmission costs. Examples of this could include remote flood sensors, mountain based seismographic sensors, and potentially weather buoys, etc.
- Mobile phones will have improved adapters for linking to computing devices such as laptops. Possible options include infrared connections, such as the current Bluestone IR industry standard

- Dedicated Internet devices will emerge, with no direct voice connection. These may evolve to personal communication devices, with higher degrees of personalisation and identity related to the individual
- Peripheral systems will evolve for devices; a classic example is a GPS plug-in, which when connected to the Internet may enable the development of personal location based information, including maps, travel direction, personalised guide books, etc. The development opportunities are huge in this space.
- Integration may be possible with applications and the CDMA Network itself. As an example, there may be scope for billing based on current cell loading, identification of the current location of the device for tailored advertising, local restaurant information delivery etc.

Network developments will come in terms of:

- Microcell implementation for wireless LAN connections internal to buildings; radio modems and network cards to become standard options for Laptops
- The public network may need to become segregated to provide Virtual Private Network capability for business communication. This could potentially take the form of applications for use over the Internet, of which this is a part, or alternatively the use of network segregation into dedicated networks.
- Segregation of microcell based systems into localised intranet networks for internal proprietary networks for LAN development. The ultimate wireless network ?
- Development of CDMA LAN networks to include interfaces to Internet offerings, i.e. through *developed e-Commerce infrastructure solutions*
- Device integration systems, such as turning the interior of a car into a “micro-network”, which would integrate communications with devices internally to the vehicle, and have consistent high power interface to external networks. This would allow the development of synergistic applications for communication between similar devices, ie parallel computing using internal wireless devices in a micro-network, and customization of car interior / facilities based on collocated devices.

The opportunities are literally limitless.

Security Issues

At EMS-Global we have identified a number of security issues that the industry will face over the next couple of years relative to the use of wireless devices. The scenarios are based around the following premise:

- The devices will be “always on”
- The devices will over time be intricately bound to the individual’s identity
- The devices will become more personalised over time
- The service offerings are immature, and are expected to become more complex over time.
- The devices will be largely mobile, with increased geographic and location independence.

The security challenges facing us over the next few years will include:

- Identity theft can occur with the theft of the device. While there may be opportunities for recovering identity through centralised management of identity mechanisms (certificate authorities), the use of another’s identity through lack of protection mechanisms cannot be discounted. The devices and underlying infrastructure must have strong user authentication mechanisms installed to prevent identity theft from becoming widespread.
- PKI infrastructures for wireless will need to be reviewed, with the likely outcome that mobile certificates will become the norm (ref www.verisign.com as an example).
- Wireless privacy issues cannot be discounted, with users expectations of privacy increasing. Sprint PCS found out the answer to that question the hard way. A spate of publicity surrounded the disclosure that its customers' mobile identification numbers were transmitted without their knowledge to Internet sites they visited via Sprint's Wireless Web service. This led to a significant backlash, and needs to be taken into account by the wireless service provider
- The devices will be “always on”, with the expectation that exploits will be developed to take advantage of that fact. Already in broadband systems such as DSL and Cable Modems, we are seeing wide-spread attacks and compromises taking place against the permanently connected devices. The recent “Denial of Service” (DoS) attacks recently are a good example of what can happen in this situation.
- The service developments and offerings are expected to be put to market extremely rapidly, and the service offerings are expected to become more complex over time. In the security space, this virtually guarantees that exploits will be developed specifically for wireless devices. What form this will take is unclear, however the current trends of DoS attacks, buffer overflows, virus attacks, and Trojans, makes problems likely in this space. We await with interest.

- Tracking unauthorized or malicious activity may become harder over time. The nature of wireless devices is that they are mobile. The use of fixed services to enable the tracking and identification of malicious activity becomes that much more difficult. New techniques and tools will be required for law enforcement and service providers to manage security, and track offenders within the new arena.
- Skills in the environment are likely to be limited, and will be difficult to source and keep. Parallels are made with the current lack of good e-Commerce and security personnel. There are opportunities for niche players to develop and market capabilities in these areas to enable industries to focus on the business issues related to wireless rather than to attempt to find limited resources.

In this paper, we have explored some of the key issues to look at in the development of mobile systems over the next couple of years. Of all the issues investigated by EMS-Global, we find that skills and knowledge in the environment are likely to be one of the key problems for industries.

Our advice is that businesses wishing to go “wireless on line”, should consult with IT providers that have a track record for delivery against complex requirements, and that can focus on these new and highly complex areas. Internal development of capability is possible to a point, however it is likely that specialist resources will be difficult to develop and retain.

In the complex issues of security, e-commerce infrastructure, and the relationship to mobile (wireless) devices, businesses and organizations will find the most efficient use of their limited funding is to use companies such as EMS-Global to provide the solutions and the capability.

EMS-Global is ideally placed to help organizations take the next step towards wireless growth, and are available to work with organizations to design and develop against their business and strategic needs. Please feel free to contact EMS-Global to discuss options, or contact us through www.ems-global.com.

References:

Sites and material referenced in this article include:

www.msn.com
www.inktomi.com
www.nokia.com
www.wirelessweekly.com
www.phone.com
www.verisign.com

Copyright

Information referenced in this paper is the sole copyright of the originating author(s). All other information and content in this article is the sole copyright of EMS-Global Limited.
