# Bluetooth Submission - 2002

| | |
|---|---|
| **Document Purpose:** | This document discusses the use of Bluetooth as a networking technology, to provide broadband communication services to mobile devices in Australia. |
| **Intended Audience:** | HOUSE OF REPRESENTATVICES<br>STANDING COMMITTEE ON<br>COMMUNICATIONS,<br>INFORMATION TECHNOLOGY & THE ARTS. |
| **Appreciation:** | I would like to thank the COMMITTEE for the opportunity to be of assistance on this subject. |
| **Document Name:** | Bluetooth Submission - 2002. |
| **Version:** | 1A. |
| **Prepared By:** | Benjamin W. Keighran. |
| **Position:** | Chief Technical Officer. |
| **Company:** | Simply Wireless. |

**THE REST OF THIS PAGE IS INTENTIONALLY BLANK**

## Contents



**THE REST OF THIS PAGE IS INTENTIONALLY BLANK**

# Bluetooth Wireless Technology

## Introduction

Bluetooth is a very advanced protocol for the transmission of data between portable devices in a secure and reliable manner.

Bluetooth, as a standard, has been around for some time and is now just beginning to be recognised by the public and industry as a reliable method for the safe transfer of information and for sheer flexibility and portability. One of the key motivators behind Bluetooth's acceptance is its very powerful and uncompromising approach to ensuring privacy and security for all users and all forms of data, video and voice traffic.

The standard specifies how mobile phones, wireless information devices (WIDs), handheld computers, and personal digital assistants (PDAs) using Bluetooth wireless components can interconnect with each other, with desktop computers, and with office or home phones.

With its use of spread-spectrum technology, the Bluetooth specification permits the secure exchange of data up to a rate of about 1.5 Mbps-even in areas with significant electromagnetic activity. With its use of continuously variable slope delta modulation (CVSD) for voice encoding, the Bluetooth specification allows speech to be carried over reasonable distances with negligible disruption.

One of the successes of Bluetooth is the rigidity of licensing of "valid" Bluetooth hardware developers, ensuring that the requirements of the standard are stringently met. Equipment that does not meet the development guidelines are not approved as fully Bluetooth compliant, reducing the likelihood of partially or non compliant equipment that could lead to the delivery of proprietary and closed solutions.

*This submission defines Bluetooth and provides examples of how it is being deployed. The examples provided are to demonstrate how Bluetooth is providing broadband communication services to mobile devices in Australia.*

**THE REST OF THIS PAGE IS INTENTIONALLY BLANK**

## Security

*Introduction*

The purpose of this section is to discuss the security of Bluetooth technology. It is not intended as a complete assessment of wireless based security, but serves to inform intending users of Bluetooth, for core and corporate applications of:

- The extent of security available to them as a part of the Bluetooth standard.
- Where any weaknesses might lie and what needs to be done to ensure protection of their intellectual property as it is broadcast across a Bluetooth network.

Throughout this section, there are broad comparisons drawn with 802.11x and other wireless standards. This is not intended as criticism, nor does it reflect on or infer any weaknesses in these other standards, but is purely to illustrate the inherent differences between Bluetooth and other more widely known forms of wireless communications.

Within the Bluetooth specification, security is dealt with at many levels:

- The Bluetooth baseband specification details a family of SAFER+ algorithms used for security procedures.
- The Link Manager specification addresses link level procedures for configuring security.
- The HCI specification details how security-related events are reported by a Bluetooth module to its host and how the host subsequently controls security.
- The Generic Access Profile covers security modes and user-level procedures for use in all products implementing Bluetohoth profiles.

The recognition of how important security is within the Bluetooth environment is demonstrated by the availability of a Bluetooth SIG white paper specifically addressing the Bluetooth security architecture. This paper suggests a framework for implementing security and gives examples of how the individual services might use these security procedures.

*Background*

Communications that are cable based are inherently secure communications and by comparison to wireless standards, they are more secure.

In contrast, since anyone could listen into a wireless transmission, the security of wireless communications systems is a key issue.

Bluetooth signals can be easily intercepted, AS CAN ANY OTHER TYPE OF WIRELESS TRANSMISSION. The difference is that whereas other wireless types are easily understood, Bluetooth signals are not broadcast sequentially on any one channel and therefore cannot be deciphered unless the "hacker" has access to equipment, the sophistication of which, parallels that of the military, before you consider the inherent encryption.

In the initial design of the Bluetooth specification, it was clearly understood by the founding members of the Bluetooth SIG (Special Interest Group), that it would be necessary to address security in advance and deliver a communications structure that is secure in itself, without the reliance on external devices (firewalls, etc.)to provide the primary security.

It was understood that the standard that was being developed would be used for secure transmissions and could be readily employed to convey personal and financial information across a wireless link. In doing so, it would have to be connected in some form, to existing networks and for this, provide an interface that would in no way reduce or compromise the existing network on the LAN.

If Bluetooth could not ensure this, then it would not be feasible as a standard.

It was decided that in order to achieve this, there was a real need for the use of built-in security mechanisms to discourage eavesdropping and spoofing (attempts to falsify the origin of the information request), independent of external systems, rather than leaving it to others, employing different standards, that might not fully serve the purpose.

As a result, link-level security features have been implemented as an integral part of the Bluetooth specification and fundamentally, Bluetooth is largely secure in itself. It is a standard with in-built traffic security.

*Security at a broad level*

The issues of security across Bluetooth 'links' are not easily discussed in isolation.

When describing how the security functions operate, network administrators are more concerned in how adding Bluetooth to their network will compromise and either enhance or degrade their existing security.

It is therefore necessary to consider the complete end-to-end structure. This involves the Bluetooth environment, the interface into the existing LAN (or VPN) and the LAN traffic itself.

In order to discuss this in entirety, the security surrounding a Bluetooth environment has to be addressed at two levels:

The Existing LAN security that is 'connected' to the Bluetooth network at application and device level from infrastructure, software and machines outside of the Bluetooth specification and security already available within the Bluetooth (SIG) specification as an inherent function of the existing specification.

Point 2 above, is further divided into:

Ensuring secure access to the Bluetooth network and preserving the integrity of the data transiting the wireless link. It is assumed that there is already existing LAN security in place and for most organisations, this will be the case.

If there is currently no LAN in place (small start-up office) then Bluetooth will provide adequate security, as a standalone system, without the need to rely on external devices.

*Existing LAN*

The Existing LAN security, it is assumed, is addressed by network administrators and managers and prevents users from gaining access to network resources within the existing Corporate network, from either an internal user or an external or wirelessly connected source. This is more an access problem and has a boundary up to and including the Bluetooth interface to the network.

Traditionally, there will be a logon server protected by its own internal OS level security and password protected security for individual users or groups of users. There is also likely to be a router acting as a firewall or in the more secure sites, separate and sometimes multiple, firewalls. Additional to this, specifically in medical and financial environments, the applications themselves might also have security systems built-in that will add yet another level of security to the overall structure.

This is the traditional network security.

Bluetooth, added to any existing network, irrespective as to whether there is an adequate and well managed security structure in place, will in no way degrade the existing security structure.

*Bluetooth*

The Bluetooth security addresses only security within the Bluetooth segment (the wireless part) and this part makes use of features *designed into* the Bluetooth specification, *when it was defined and ratified.*

This is NOT an added security feature, it is an inherent part of the accepted international standard, built into the standard.

Bluetooth totally secures the link between the user and the LAN interface.

After authorising access to the LAN for valid users, the Bluetooth devices make no further checks on access security. This is why it is important that a security plan already exists for the LAN and network administrators do not rely purely on Bluetooth for authentication. With ANY wireless system, separate authentication processes are always recommended.

The primary security features inherent to Bluetooth are Authentication, Encryption and Frequency Hopping.

Within each of these key points, there is a very comprehensive structure of features that overlap and co-operate with each other to provide a very secure wireless environment.

One feature certifies access by authorised users only, the next preserves the integrity of the data travelling wirelessly and the last feature makes eavesdropping even more difficult, albeit impossible.

Together, they form a formidable barrier to hackers.

Authentication prevents spoofing (unauthorised users pretending to be someone else) and unwanted access by unauthorised users, to critical data and functions.

It is essential to understand, however, that the security architecture of the Bluetooth specification is hardware based and will only authenticate devices, not users. This means that a trusted device that is stolen or borrowed can be used as if it were still in the possession of the rightful owner.

Enforcing security at only this basic level should be limited to the user-friendly, public-oriented usage models, such as discovering services and exchanging virtual business cards. Network administrators who employ only this level of security to their networks, cannot be serious about protecting their networks.

If there is a need for user authentication, supplementary application-level security methods MUST be employed, such as the entry of a username and password, particularly with such applications as mobile e-commerce.

Because there will be differing demands on data security, applications and devices must have more flexibility in the use of link-level security. To meet these differing demands, the Bluetooth specification defines three security modes that cover the functionality and application of devices.

Security is important not only to ensure the privacy of your messages and files as they fly through the air, but to ensure the integrity of electronic commerce transactions as well. Accordingly, the Blue-tooth specification also offers a

flexible security architecture that makes it possible to grant access to 'trusted' devices and services with-out providing access to other 'untrusted' devices and services.

Encryption uses an established key structure for the conversion of cleartext to ciphertext and vice versa, between end devices, presenting to any eavesdropper, a garbled string of essentially random 'bits', securing the Bluetooth link and ensuring privacy. It can be argued that these can be broken and the information decrypted, but in general, the algorithms are very difficult to crack without the use of sophisticated processing equipment and the time taken to 'discover' the encryption key is generally longer than the validity period of the information being transmitted.

In addition, Bluetooth wireless technology includes session-key generation that can be changed at any time during a connection. Even in the unlikely event that a hacker is able to grab a connection, he or she will not be able to stay on a piconet for any length of time.

Bluetooth encryption is based on a variation of the SAFER+ cipher used to authenticate devices. Designed by Cylink Coropration as a candidate for the U.S. Advanced Encryption Standard (AES), it is now available in the public domain.

In a piconet, all the devices know the master's slot clock and basic device address. The secret key for encryption varies. When a communication is to occur, a device will try to verify that it shares a secret key with another device it wants to communicate with. The verifying address cannot just ask for the key to be transmitted, or it could be eavesdropped. Instead the verifying user sends a random number to the requestor and asks them to encrypt the number with the secret key and return the encrypted key to the verifier. The verifier then checks the random number using the secret key and if there is a match, assumes that both sides have the same key. The message interchange can then take place.

The Bluetooth specification uses a key length of between 1 and 16 octets (8 and 128 bits). For key lengths less than 128 bits a modulo 2 operation is used to reduce the key length. The reduced key is then encoded using a block code so as to more uniformly distribute the starting states of the encryption sequence.

In addition to the link-level functions, Bluetooth uses a frequency-hopping system with the spread-spectrum signal, both to reduce interference with transmissions from the same Bluetooth antenna and to make locking onto and tracking the signal extremely difficult. Bluetooth employs a very high speed pseudo-random frequency hopping algorithm to control the hopping. The key generated to be used by the algorithm depends upon a number of factors, including the address of the devices in the actual conversation. The Bluetooth specification calls for the transmitter to perform 1600 hops per second across 79 different frequency bands jumping from one frequency to the next at a specific hop rate in accordance with a pseudorandom code sequence.

The order of frequencies selected by the transmitter is taken from a predetermined set dictated by the code sequence. For example, the transmitter may have a hopping pattern of going from the ninth frequency band, to the twelfth frequency band, to the twentieth frequency band, and so on across the entire range of available frequencies. The receiver device tracks these changes. Since only the intended receiver device is aware of the transmitter's hopping pattern, only that receiver can re-assemble and make sense of the data being transmitted. All other data streams to other devices are totally unintelligible.

The FCC mandates that frequency-hopped spread-spectrum systems not spend more than 0.4 seconds on any one channel each 20 seconds, or 30 seconds in the 2.4 GHz band.

Furthermore, they must hop through a range of at least 50 different channels if using the 900-MHz band, and 75 different channels in the 2.4-GHz band. These rules reduce the chance of repeated packet collisions in areas with multiple frequency-hopping transmitters. The Bluetooth specification, even more stringent, specifies a rate of 1600 hops per second among the 79 frequency bands within the ISM band.

In accessing the degree of security this offers, it should be noted that the U.S. military considers a communications link using frequency hopping over 79 channels, in a unique random pattern, to be totally secure within itself.

All Bluetooth units participate in a piconet, with each unit sharing a common channel. Up to eight interconnected devices can be supported by a piconet, comprising one master and up to seven slaves. This relationship remains in place for the duration of the piconet connection.

The units that participate in a piconet are time and hop synchronized to the same channel. Every Bluetooth unit has an internal system clock, which determines the timing and hopping used by its transceiver. The timing and frequency hopping on the channel of a piconet are determined by the clock of the master.

When the piconet is established, the master clock is communicated to the slaves. Each slave adds an offset to its native clock, based on its unique address, to align with the master clock. Since the clocks are free running, the offsets have to be updated regularly.

Other frequency-hopping transmitters in the vicinity will be using different hopping patterns and much slower hop rates than Bluetooth devices. Should transmitters that do not use Bluetooth wireless technology coincidentally attempt to use the same frequency at the same moment, the data packet transmitted by one or both devices will become garbled in the collision, and a retransmission of the affected data packets will be required. A new data packet will be sent again on the next hopping cycle of each transmitter.

Another factor adding to the security is the limited transmission range of devices using Bluetooth wireless technology. In general, devices separated by more than 100 metres cannot communicate. Unauthorised eavesdroppers outside of this range will also not be able to communicate.

It is possible, again with the use of sophisticated listening equipment, to 'sense' transmissions from a greater distance, but this equipment is highly specialised and must seek to isolate a specific device to device transmission, possibly encrypted and hopping all over the available spectrum. As this equipment is largely military in its nature, it is recommended that those people who would have information that would be so secure as to encourage the possible use of these devices against them, would take other precautions to secure their databases.

It should be noted, in defence of Bluetooth, that the electrical transmissions from network cables and telephone cables (remote communications) are far higher and more easily intercepted than Bluetooth transmissions, do not hop frequency and are rarely encrypted.

The most important outcome from all of this, is the fact that in order to properly address the security features of Bluetooth communications, it is necessary to demonstrate that within Bluetooth, security has been seriously thought about during the design. As a result there is more than one level of security available to the users of Bluetooth.

Many manufacturers, recognising the promise of Bluetooth and its particular attention to security, are currently developing specific devices for advanced portable banking.

Nokia and Ericsson are among companies advancing the idea of using phones and palmtops, equipped with Bluetooth wireless technology, as 'personal trusted devices". Using these, consumers can load 'money' into an electronic wallet at an automated teller machine (ATM) and pay for merchandise at the point of sale, with the same device, whether at a retail store or a vending machine.

*Security summary*

Bluetooth has been totally designed by people who are entrenched within the communications industry, unlike the 802.11x standards which have been designed by companies who "specialise" in data based computing networks.

Developed as a totally new and refreshing look at the need for portable communications and computing, Bluetooth has been driven by mobile phone manufacturers who have a definite interest in lower powered implementations of greater flexibility and simplicity and with a definite need to ensure the privacy of all those who use it.

One of the most significant issues that has been described in the Bluetooth specification is the security of the communications. Designed to handle not only voice, but also data and video, the privacy and security required to ensure this is extremely complex, but must also be simple to operate and cause minimal overheads to the user.

The Bluetooth security structure is so complex and sophisticated that a complete specification document is required to adequately address all aspects of its implementation. Of all wireless based specifications, it is the most stringent, involving multiple, overlapping security systems that collectively provide a formidable collection of barriers to the prospective hacker.

Of most importance, these are highly formidable, but yet they are implemented in such as way so as to be totally transparent and of no impact to the user, while operating to secure all transactions passing across the Bluetooth interface. Hidden, as it is, inside the protocol, the Bluetooth security is far harder to access and therefore, compromise.

**THE REST OF THIS PAGE IS INTENTIONALLY BLANK**

## General Uses & Applications

This section does not define Bluetooth or show how Bluetooth is providing broadband communication services to mobile devices in Australia. The purpose of this section is to outline how Bluetooth is being used by the General Public at present.

Following are brief descriptions demonstrating how Bluetooth is currently connecting people:

Combination: *Bluetooth enabled Laptop and PDA*

Usage: Wirelessly sync programs on the Laptop such as MS Outlook with PDA, Wirelessly share Laptop internet connections with PDA.

Combination: *Bluetooth enabled Laptop and Phone*

Usage: Wirelessly sync programs on the Laptop such as MS Outlook with Phone, Laptop can use the Phone as a Wireless modem to connect to the internet (This may be through a dial-up connection or GPRS), Send SMS's from Laptop, Send & receive faxes from Laptop.

Combination: *Bluetooth enabled PDA and Phone*

Usage: PDA can use the Phone as a Wireless modem to connect to the internet (This may be through a dial-up connection or GPRS), Initiate phone calls, Send SMS's, Receive FAX's.

Combination: *Bluetooth enabled Phone and Headset*

Usage: Calls can be received and initiated from the Headset via the phone.

**THE REST OF THIS PAGE IS INTENTIONALLY BLANK**

# Bluetooth Scenarios

## Introduction

This section describes four scenarios of how Bluetooth is being used by companies such as Simply Wireless, to provide broadband communication services to mobile devices. It also highlights how Bluetooth is one of the key technologies that can make the mobile information society possible, blurring the boundaries between home, the office, and the outside world.

As more and more manufactures adopt Bluetooth and create devices that support it, there will be a larger requirement for Bluetooth environments. The scenarios below are examples of some of the experiences the public will have when they are connected via Bluetooth to broadband services.

Together with other industry initiatives and broadband Bluetooth environments, Bluetooth will have tremendous effects on everyday life.

**THE REST OF THIS PAGE IS INTENTIONALLY BLANK**

## Shopping Scenario

Everybody loves to shop, but few of us have the time to walk around Shopping Malls, hoping to find products that meet our needs. Now everyone has time to shop!

You are looking to buy a new DVD player, so you visit your local Shopping Mall.

When you arrive at the Mall, the Mall's server recognises you are a regular shopper and updates your loyalty shopper status. The Mall's server also sends information to your mobile phone/PDA informing you of current specials and sales that are taking place in the Mall.

You use your PDA to search the range of stores that sell DVD players. When you complete your search, a highlighted route map appears on your PDA and navigates you to the stores that stock your selected items.

You enter a store and see a DVD player that interests you, however there is not a Sales person around to help you. With your PDA there is no need to wait for a shop assistant. You use your PDA to access the stores server, which gives you direct access to manufacturers, technical information, price, warranty and stock availability. Despite having a range of DVD players, they do not have one that meets your exact needs.

As you walk out of that store the Mall server sends a message to you that your friend has just entered the mall. You send a message to your friend, via your PDA, asking her to meet you for lunch at "Café Blue" During lunch you receive an instant message from Sanity Records on your PDA explaining they are having a clearance sale. You use your PDA to access pictures and technical information on their full range of products, whilst at the same time you listen to the TOP 10 singles on sale. You find a DVD player that is just perfect and it's on sale, however you notice that it is the only one left in stock. You use your PDA to put the DVD player on hold, so you can go and take a look at it after lunch. You relax and continue your lunch, knowing that your DVD player is on hold, and will be there when you finish.

After lunch you decide to check out the DVD player. The DVD player is exactly what you are looking for, so you purchase it electronically, via your PDA. Payment is instant, receipts are sent to your home email account. On your way out of the shop you use the Mall's server to link to the internet and access the web page of your local Video Ezy Store to get a DVD to watch on your new player. You notice that they have 2 copies of 'Toy Story 3' in store. Using your PDA you book your DVD, which you pick up on your way home.

**THE REST OF THIS PAGE IS INTENTIONALLY BLANK**

## Real Estate Scenario

You arrive in the office after a busy morning out on the road. The office Bluetooth network automatically picks up the Hand Held Computer/PDA you carry, and immediately begins to synchronise and update all data between your office PC and your PDA. All forms, payments, emails, appointments, database information and contracts are synchronised. Even the morning newspaper and financial review are downloaded. With all this being taken care of, you are able to focus on the meeting with a client, you are just about to walk into.

During the meeting the client asks for information regarding a certain property that is currently for sale. You use your PDA to surf the corporate intranet and locate the relevant information. The client requests a copy of the relevant documents. You send a copy of all documents to the printer at reception via your PDA, so that the client can pick them up on his way out of the meeting. You also send a copy of the documents to the client's email address via your PDA, so that it is waiting for him at his office.

After the meeting you pass a colleague (Mr Blue) in the hall. He requests a copy of a contract you are currently working on. You use your PDA to access the contract and send it directly to his PDA via Bluetooth (PDA to PDA). You then ask Mr Blue if he could help one of your residential clients find a commercial property. He agrees, and you send him the contact details and history of the client which simultaneously synchronises from your address book to his address book (PDA to PDA).

Whilst this is happening, the Bluetooth office network is synchronising with your PDA and updating all information via a "2 way" synchronise. On the way to your desk you receive a mobile phone call. It is the solicitor of your client you visited this morning, he updates you with information regarding the proposed purchase of the property and proceeds to give you his contact details. As you are walking down the hall, you do not have paper and a pen. You choose to hit the voice memo switch on your PDA. As he gives you his contact details, you repeat them as if you were writing them down. Using voice recognition, your PDA writes down the contact details and records a voice note for later playback.

Your Boss comes to your office to discuss budgets. Whilst you are in the meeting, your secretary takes a call from a client, who requests a meeting with you for 10.00am 27 June 2001. Because you are in a meeting, she accesses your electronic diary directly, which is constantly synchronising with your (PDA) that is in your pocket. She notices that only seconds before, you scheduled a meeting for this exact time. She reschedules another time with the client and at the same time sends a message to your diary to alert you that an appointment has been made for you.

**THE REST OF THIS PAGE IS INTENTIONALLY BLANK**

## Car Dealership Scenario

There's nothing like the buzz you get from walking into a car showroom knowing that today is the day you're going to buy that 4-by-4 you've been dreaming of. But how quickly that excitement can turn to frustration when the salesman disappears and you're left to kick your heels (or tires!). At the end of a lengthy wait, it turns out he can't get hold of the information you need and they've even run out of brochures.

Now let's run through the same scenario in a Bluetooth enabled world...

The sun is shining and the air is crisp. You stride into the forecourt of your nearest car dealership and are greeted by a cheery, "Good Morning, Mrs Jones!" (The garage's Bluetooth network has picked up your details from the personal device you carry and immediately transferred it to the salesman's screen.)

He quickly shows you to a suitable display model – no forms to fill in now, of course – and you have plenty of time to focus on the car itself. Sleek shape, powerful engine, plenty of room inside, "but what about the trim?" you ask. "I like leather, but beige doesn't wear well in our family. What are my options?"

Amazingly, this doesn't precipitate a trip to the back room and cup of tea while you wait, instead the salesman looks at his personal digital assistant (PDA). He can access all of the information held on his company's database instantly, whilst still sitting in the car beside you. Alternatively, if you need more time to think and prefer a bit of personal space, he can log you into the company intranet as a guest, leaving you to browse all of the options on your own PDA or WAP phone.

Your mind is made up, you're happy with this model but you really want metallic gray. This time the salesman needs to query head office for availability and an estimated delivery date. Again, he can complete the entire inquiry without picking up a phone. He's a good guy, in fact he's clinched the sale by promising you a 10% discount, and he receives final permission for the deal on his PDA while you exchange toddler anecdotes.

The scene moves on: It's several months later and you've received a service-reminder email from the garage on your WAP phone.

As you draw up on the forecourt, the garage's Bluetooth network detects your Bluetooth service card, instantly checking you in. The customer service rep greets you with a Diet Coke -- your favourite drink -- and the keys to your courtesy car, having read off the information from her screen. Because the car is equipped with Bluetooth components, it can be remotely diagnosed and given a first-level health check without the engineer leaving his desk.

It's nearly midday and, having stocked up on some shopping, you arrive home in the courtesy car. Back at the garage, the engineer has already read the health check results, checked inventory for new parts and ordered them up from the storeroom, all whilst he is under the bonnet of your car. His report, which he fills out direct onto his service tablet, is transferred via Bluetooth onto the company's service database and a copy awaits you, together with the car keys, when you return later that same day.

And when you decide it's time for a change of car, the process only gets easier. You've chosen to receive regular updates on new models that might appeal, via your personal device, and you know you can call up a test-drive schedule on your WAP phone whenever you like. Add to that, the fact that the garage has given you on-line access to national trade-in information from your personal device and you're in a great position to choose the car you want fast.

Bluetooth technology – it puts you in the driving seat.

## Airport Scenario

To most people flying today means: waiting, queuing, wasting time.

All that is about to change, thanks to a powerful combination of Bluetooth technology.

Take a look at how things will be…

Right from the moment you arrive at the airport you will experience the benefit.

A welcome message appears on your personal digital assistant (PDA) or mobile WAP phone, check-in is automatic – no queues, no fumbling for tickets – your electronic ticket is automatically validated via the Airport's secure Bluetooth network.

As you leisurely make your way to the Airline business lounge relevant information such as boarding times, gate numbers and yes, unfortunately airline delays, can be sent to your PDA.

You may also have chosen to receive details of special offers from the various duty-free stores.

At the business lounge, entry is automatic. Through your Bluetooth enabled PDA you are recognized as a valued frequent flyer and receive the level of service you deserve, your points status is displayed and you find out you got an upgrade. If time permits, you may wish to order food and drinks from the selection displayed on your PDA.

In the lounge it is time for you to decide what to do, the world is at your fingertips. You may want to work - you can access your office computer via a secure virtual private network (VPN).Picking up emails, reviewing and changing diary schedules, in fact, do most things you could as if you were in the office. You may want to browse the Internet – check out what the competition are doing, read up on your new customer prospects. You may want to make changes to your travel arrangements – review your hotel, check on your hire car. All of these things can be done from your Bluetooth enabled device (PC, PDA, phone, you choose).

And while you're busy doing these things you don't have to worry about missing your plane – important flight information will be continually sent to you.

At the gate, boarding is as simple as check-in. "Enjoy your flight!"

This flight of the future is not so far away. Bluetooth enabled devices can automatically sense each other, allowing instant two-way communication. Internet, WAP, Intranet surfing and messaging using Bluetooth technology are all here today.

So this is no flight of fancy. Using Bluetooth enabled devices over a Bluetooth network is set to change air travel for the better.

**THE REST OF THIS PAGE IS INTENTIONALLY BLANK**