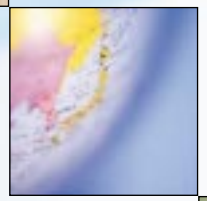
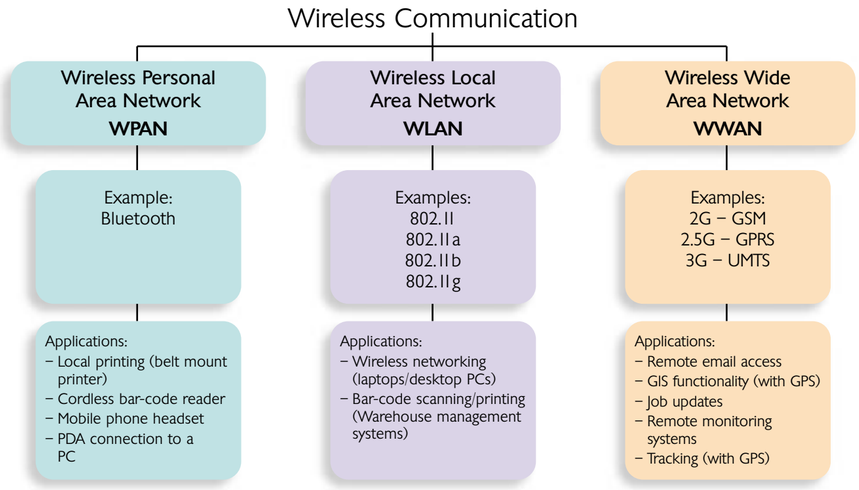


spirit
DATA CAPTURE LTD

Guide to Wireless Communication

Welcome

Welcome to the Spirit Data Capture Guide to Wireless Data Communication. We hope that you find it useful. We have divided it up into sections – so that you can easily find the relevant information.



Wireless Personal Area Network (WPAN)

Wireless Personal Area Networks operate immediately around a person or device. Typically, they operate within a 10 metre range. A common example of the technology used to create a WPAN, is Bluetooth.

An introduction to Bluetooth

Harald Bluetooth was king of Denmark in the late 900s. He united Denmark and part of Norway into a single kingdom. Choosing his name for the standard, indicates how important companies from the Baltic region are to the communications industry.

Bluetooth is a radio-frequency standard. It was developed by a group of electronics manufacturers – to allow any sort of electronic equipment (computers, mobile phones, keyboards, printers, headphones, remote controls, etc) to make connections without wires or cables. Companies belonging to the Bluetooth Special Interest Group or SIG (well over 1,000 of them), see Bluetooth radio taking the place of wires for connecting anything that needs to send or receive data from anything else.

There are numerous ways that devices can connect to one another. For example:

- A personal digital assistant (PDA) to a PC, via a USB cable and a docking cradle
- Television to video, with SCART or coax cables
- Hi-Fi units can connect with a multitude of cables (phono, fibre, Neutric, copper)

Virtually none of the above will connect using the same types of cables or connectors, as there are differing standards and sizes at play.

The clearly defined standards of Bluetooth, mean that a Sony mobile phone will work quite happily with a Plantronics headset. The phone and headset don't care who has manufactured them, only that they can connect to a like device.

From a user's point of view, here are the key benefits of Bluetooth:

1. It's wireless.
2. When you travel, you don't have to worry about taking any cables with you.
3. You don't have to think about it – as Bluetooth doesn't require you to do anything special to make it work. When switched on, the devices find each another and strike up a connection. Voila! Job done.
4. It's inexpensive.

The way we connect things is becoming increasingly more complex. It sometimes looks as though your home or office is being taken over by cabling. This not only looks unsightly, but it also harbours dust and can be a safety hazard if not carefully installed.

Bluetooth – how it works

Bluetooth communicates on a frequency of 2.45 gigahertz. Some devices that are already in use may also use this same radio-frequency band. For example, the latest generation of cordless phones, some baby monitors, and headsets all make use of frequencies in the ISM band. Ensuring that Bluetooth enabled devices and other devices using the same RF band don't interfere with each another, has been included in the design principles.

To avoid interference with other systems, Bluetooth devices operate on a very low power of 1 milliwatt. In comparison, some mobile phones can transmit in hundreds of milliwatts. This low power limits the range of a device to around 10 meters. However, even with the low power, the walls in your house/office won't stop the signal completely. Brick walls will reduce the signal, but the signal will still travel.

Bluetooth®

With the possibility of many different Bluetooth devices in close proximity, you may think they would interfere with each other. However, in reality this is unlikely. Bluetooth uses a technique called spread-spectrum frequency hopping (from pre 802.11 days). This enables the device to transmit on 79 random frequencies. Because the Bluetooth system changes frequencies 1,600 times a second, it means that many more devices can make full use of the available radio frequencies.

Every Bluetooth transmitter frequency-hops automatically, making it extremely unlikely that two will be on the same frequency at the same time. In addition, Bluetooth minimises disruption with telephones, baby monitors, garage openers etc., because interference on a particular frequency will only last for a fraction of a second.

When Bluetooth devices come within a range of one another, an automatic electronic exchange takes place. This is primarily to establish if they are of a compatible type; have data to share; or one needs to control the other. The user does not have to take any action, as the connection should happen within a few seconds.

Once this electronic exchange has occurred, the devices will have formed a small network, called a personal area network (PAN or piconet). This PAN may fill a room (depending on the devices) or be no more than the distance between the mobile phone in your car and your headset. The members randomly hop frequencies in unison, so that they stay in touch with one another and avoid other piconets that may be operating in, say, the car next to you.

To simplify things further, within a normal home environment, you may have a Bluetooth enabled Hi-Fi, DVD player, satellite box, TV, cordless telephone and a personal computer (not all of these are Bluetooth enabled yet, but they soon will be). When switched on, each of these systems forms its own piconet to communicate between the main unit and whatever it needs to control.

The cordless telephone has one Bluetooth transmitter in the base and another in the handset. The transmitter will have been programmed with an address that falls into a range of addresses it has established for a particular type of device. When the base is first turned on, it sends radio signals asking for a response from any units with an address in a particular range. Since the handset has an address in the range, it responds and bingo! a tiny network is formed. From then on, even if one of these devices receives a signal from another system, it will ignore it, since it is not from within the network. All the other systems perform similar routines, establishing networks among addresses in ranges pre-set by the manufacturers.

Bluetooth is a radio-frequency standard and allows any sort of electronic equipment (computers, mobile phones, keyboards, printers, headphones etc) to make connections without wires or cables.

Once the networks are established, the systems begin talking among themselves, each one hopping randomly through all available frequencies. Because each network is changing the frequency of its operation thousands of times a second, it's very unlikely that any two or more networks will be on the same frequency at the same time. If they are, then the resulting collision will only cover a tiny fraction of a second, and special software designed to look for these instances, will remove any corrupted information.

Bluetooth security

There are some known issues with Bluetooth security and the following is the minimum you should address:

- Avoid the use of unit keys.
- Use combination keys.
- Perform bonding in an environment that is as secure as possible against eavesdroppers.
- Use long random Bluetooth passkeys.

Bluetooth Specifications

The system can send data at more than 64,000 bits per second in a full-duplex link. This is more than high enough to support many voice connections. In a half-duplex link (a printer for example), Bluetooth can transmit up to 721 Kbs/second in one direction and 57.6 Kbps in the other. If the same speed in both directions is required, the capacity will be 432.6-Kbps in each direction.

The devices in a piconet share a common communication channel. The channel has a total capacity of 1 megabit per second (Mbps). Headers and handshaking information consume about 20 percent of this capacity.

In the United States and Europe, the frequency range is 2,400 to 2,483.5 MHz, with a total of 79 1-MHz radio frequency (RF) channels. Most devices use the range 2,402 MHz to 2,480 MHz.

Japan uses the frequency range 2,472 to 2,497 MHz and 23 1-MHz RF channels.

A data channel hops randomly 1,600 times per second between the 79 (or 23 if you are in Japan) RF channels. Each channel is divided into time slots 625 microseconds long.

A piconet has a master and up to seven slaves. The master transmits in even time slots, slaves in odd time slots. Packets can be up to five time slots wide. Data in a packet can be up to 2,745 bits in length.

There are currently two types of data transfer between devices: SCO (synchronous connection oriented) and ACL (asynchronous connectionless).

In a piconet there can be up to three SCO links of 64,000 bits per second each. SCO links use reserved slots set up by the master. They can support up to three SCO links with one, two or three slaves. Slots not reserved for SCO links can be used for ACL links. One master and slave can have a single ACL link. ACL is either point-to-point (master to one slave) or broadcast to all the slaves. ACL slaves can only transmit when requested by the master.

Wireless Local Area Network (WLAN)

A WLAN enables a mobile user to connect to a Local Area Network through a wireless radio connection. High speed wireless LAN networks are now available and can be implemented quickly and at low cost. There are a range of standards which specify the technology for WLAN, including 802.11 a, b and g.

What is 802.11a, b and g?

Let's start with some history. The origins of 802.11 wireless can be traced back to the early 1940s . In 1942, Hollywood actress, Hedy Lamarr, patented the basic principles of modern Spread Spectrum technology. The frequency-switching system for torpedo guidance was two decades ahead of its time. Her original concept was based around 88 channels – the same number of keys as on a piano – and formed the basis of the 802.11 wireless systems we use today.

During the 1950s the military began to develop the technology, using (at the time) modern electronics. By the 1960s spread spectrum radio had become a satellite communications technology. Encrypted data links were used by many national intelligence services. It is only during the last ten to twelve years, that spread spectrum radio devices have migrated into everyday life - in cordless phones, burglar alarms, wireless local loops (WLL), and wireless local area networks (WLANs).

Standards

Standards are important, as they generally encourage manufacturers to design products that are open standard compliant. Although this does not always mean that all manufacturers will follow the standards.

It can still be frustrating when one manufacturer's equipment will not work consistently with another manufacturer's!

Originally, there was no common standard for spread spectrum radio devices. As recently as the early 1990s, there were any number of different methods of using this technology. However, none were interoperable. The two well known ones were FHSS (Frequency Hopping Spread Spectrum) and DSSS (Direct Sequence Spread Spectrum). FHSS was the slightly more secure method, although only marginally.

Towards the end of the 1990s, the IEEE (Institute of Electrical and Electronic Engineers) developed the 802.11b standard, which has helped define the 802.11 radio system we have today.

The 802.11b committee of the IEEE develops standards for Local and Wide Area Networks. For example, the 802.3 committee develops standards for Ethernet-based wired networks, the 802.15 group develops standards for personal area networks, and the 802.11 committee develops standards for wireless local area networks (LAN).

802.11 further defined

802.11a is a different standard for wireless LANs operating in the 5 GHz frequency range – with a maximum data rate of 54 Mbps.

802.11b, or Wi-Fi, is a standard for wireless LANs operating in the 2.4 GHz spectrum with a bandwidth of 11 Mbps.

802.11g, is for WLANs operating in the 2.4 GHz frequency – but with a maximum data rate of 54 Mbps.

Many of the systems deploying the 802.11g standard, also include support for 802.11b as both 11Mb and 54Mb devices run on the same frequency. Some suppliers even incorporate bespoke software that allows transmission at higher data rates. This will only work if all the systems are from the same manufacturer. Generally, it is better to avoid using these special software settings as the results can be unpredictable.

Other task groups of the IEEE are working on enhanced security (802.11i), spectrum and power control management (802.11h) and quality of service (802.11e).

802.11b security

The following are examples of some of the potential security threats for WLAN networks:

Eavesdropping (disclosure of data)
Eavesdropping on network transmissions can result in the disclosure of confidential data, unprotected user credentials, and identity theft. It also allows sophisticated intruders to collect information about your IT environment, which can be used to mount an attack on other systems or data that might not otherwise be vulnerable.

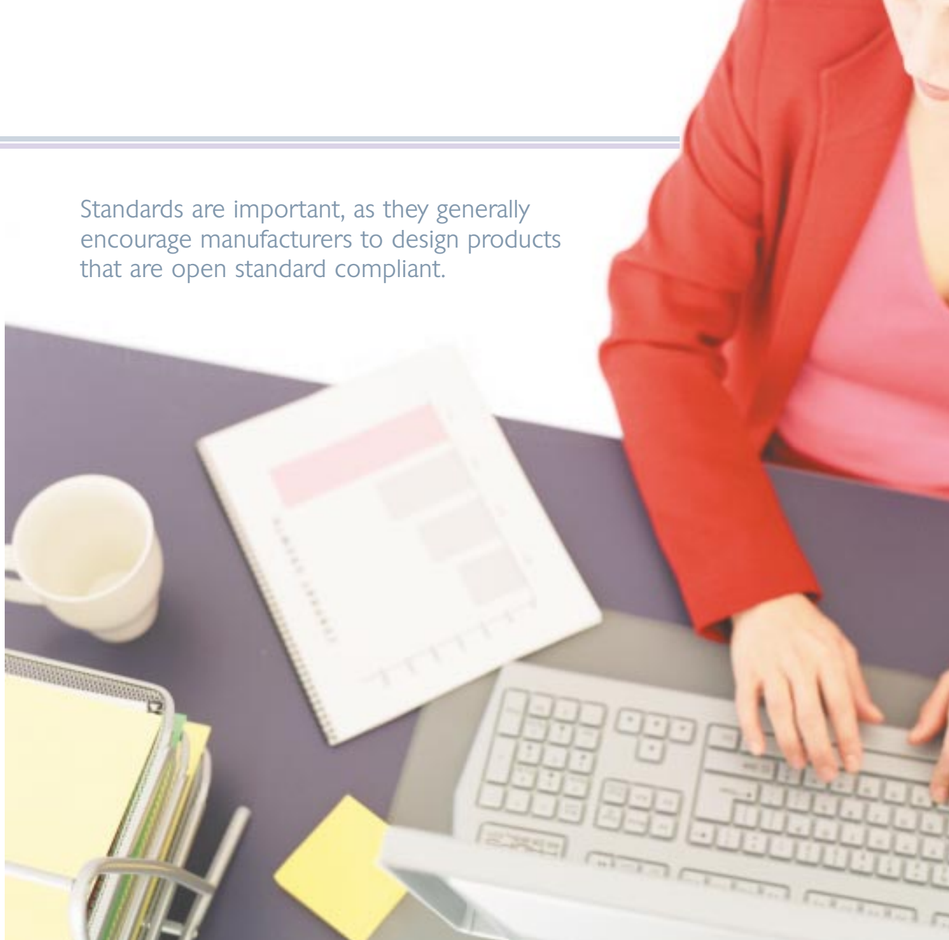
Interception and modification of transmitted data

If an attacker can gain access to the network, they can insert a rogue computer to intercept and modify network data communicated between two legitimate parties.

Spoofing

Ready access to an internal network allows an intruder to forge apparently legitimate data in ways that would not be possible from outside the network. For example, a spoofed email message. People, including system administrators, tend to trust items that originate internally far more than something that originates outside the corporate network.

Standards are important, as they generally encourage manufacturers to design products that are open standard compliant.



Denial of service (DoS)

A determined assailant may trigger a DoS attack in a variety of ways. For example, radio level signal disruption can be triggered using something as low tech as a microwave oven. There are more sophisticated attacks that target the low level wireless protocols themselves, as well as less sophisticated attacks that target networks by simply flooding the WLAN with random traffic.

Free–loading (or resource theft)

An intruder may want nothing more sinister than to use your network as free point of access to the Internet. Though not as damaging as some of the other threats, this will, at the very least, not only lower the available level of service for your legitimate users – but may also introduce viruses and other threats.

Accidental threats

Some features of WLANs make unintentional threats more real. For example, a legitimate visitor may start up a portable computer with no intention of connecting to your network. However, they may then be automatically connected to your WLAN. The visitor's portable computer is now a potential entry point for viruses onto your network. This kind of threat is only a problem in unsecured WLANs.

Rogue WLANs

If your company officially has no WLAN, you may still be at threat from unmanaged WLANs springing up on your network. Low priced WLAN hardware bought by enthusiastic employees can open unintended vulnerabilities in your network, especially if no steps are taken by the employee to install basic security measures. Most suppliers of hardware have a standard SSID (and no other security enabled). Most hackers will know that almost all new users (and some who should know better) don't bother to change basic 'out of the box' settings.

Protecting your radio network

Nothing is totally secure and those that tell you otherwise are fooling themselves and you. However, you can protect your network by making it more difficult to gain access.

There are a few simple ways to afford protection from unauthorized use of a radio network. The most obvious is to change ALL the standard settings on your chosen equipment to something only you know. A pretty obvious statement, but one that many people don't think of. This is so easy to achieve and does not take too long, once the basic principles are understood. The absolute minimum would be:

- Change the SSID. This is the first thing your Access Point uses to allow registration. Most unscrupulous individuals will know all the standard settings. Even though they may not do any lasting harm on your network, don't give them the opportunity to gain access! You won't know they are there but they could cause you slow response times and they can even gain access to sensitive information.
- Use a 128 bit (or higher) WEP (Wireless Equivalency Protocol) key or multiple keys if your hardware allows it. Most do, as this is a way to stop authentication to your AP.
- Reduce the coverage of your AP by lowering the radio power – so that coverage is contained within the confines of your property. However, not all devices designed for the SOHO or home user allows this and you may find, if you want this feature, you'll have to spend a bit more at the outset. All Cisco and other industrial units will offer this option plus some 'bespoke' settings.

There are other ways in which security can be tightened. However, they do come at a cost which can be prohibitive, unless the data and restricted access on your network warrants it.

The most important thing to remember is to WRITE DOWN all the settings you change, and what they are changed to. If you forget or you have a problem of some kind, or just want to add another device, it will be very difficult, if not impossible, to configure without this information.

Wireless Wide Area Network (WWAN)

Wireless Wide Area Networks (WWAN) provide access to information anytime and anywhere where there is cellular (data) coverage. This means that you can send and retrieve emails, browse the internet and access other corporate information while you are away from the office. Wireless WANs cover a much more extensive area than wireless LANs. They are generally used to enable the mobility of the entire network or bridge branch offices of an entire company.

How does it work?

In wireless WANs, communication occurs predominantly through the use of radio signals over analog, digital cellular, or PCS networks. However, signal transmission through microwaves and other electromagnetic waves is also possible. Today, most wireless data communication takes place across 2G Cellular systems (the term used to describe the current GSM second generation digital network technology.)

The traditional analog networks were originally designed for voice rather than data transfer and have some inherent problems. However 2.5G (GPRS) and the new 3G digital cellular networks are fully integrated for data/voice transmission. With the advent of 3G networks, transfer speeds should also increase greatly.

WWAN connectivity requires wireless modems and a wireless network infrastructure, provided as a fee-for service, by a wireless service carrier. Portable devices receive communications as the connected wireless modems and wireless networks interact via radio waves. The modem directly interfaces with radio towers, which carry the signal to a mobile switching centre, where the signal is passed on to the appropriate public or private network link (i.e., telephone, other high speed line, or even the Internet).

2G – GSM

GSM (Global System for Mobile communication) is a digital mobile telephone system. It is widely used in Europe and other parts of the world. GSM uses a variation of time division multiple access (TDMA) and is the most widely used of the three digital wireless telephone technologies (TDMA, GSM, and CDMA). GSM digitizes and compresses data, then sends it down a channel with two other streams of user data, each in its own time slot. It operates at either the 900 MHz or 1800 MHz frequency band.

GSM is the de facto wireless telephone standard in Europe. According to the GSM MoU Association, GSM has over 120 million users worldwide and is available in 120 countries. Since many GSM network operators have roaming agreements with foreign operators, users can often continue to use their mobile phones when they travel to other countries.

American Personal Communications (APC), a subsidiary of Sprint, is using GSM as the technology for a broadband personal communications service (PCS). The service will ultimately have more than 400 base stations for the palm-sized handsets that are being made by Ericsson, Motorola, and Nokia. The handsets include a phone, a text pager, and an answering machine.

GSM, together with other technologies, is part of an evolution of wireless mobile telecommunication that includes High-Speed Circuit-Switched Data (HCSD), General Packet Radio System (GPRS), Enhanced Data GSM Environment (EDGE), and Universal Mobile Telecommunications Service (UMTS).

2.5G – GPRS

GPRS is a packet-based wireless communication service. Data rates are typically 56 Kbps and and allows continuous connection to the Internet for mobile phone and computer users. The higher data rates allows users to take part in video conferences, interact with multimedia websites and similar applications using mobile handheld devices as well as notebook computers.

The GPS (Global Positioning System) is a ‘constellation’ of 24 well-spaced satellites that orbit the Earth

Wireless Wide Area Networks (WWAN)

GPRS is based on Global System for Mobile (GSM) communication. It complements existing services such as circuit-switched cellular phone connections and the Short Message Service (SMS).

GPRS packet-based services should cost users less than circuit-switched services. This is because communication channels are being used on a shared-use, as-packets-are-needed basis rather than being dedicated only to one user at a time. It should also be easier to make applications available to mobile users, because the faster data rate means that middleware (currently needed to adapt applications to the slower speed of wireless systems), will no longer be needed. As GPRS becomes available, mobile users of a virtual private network (VPN) will be able to access the private network continuously – rather than through a dial-up connection.

GPRS also complements Bluetooth. In addition to the Internet Protocol (IP), GPRS supports X.25, a packet-based protocol that is used mainly in Europe. GPRS is an evolutionary step toward Enhanced Data GSM Environment (EDGE) and Universal Mobile Telephone Service (UMTS).

3G – UMTS

3G is the third-generation wireless technology. It refers to the latest developments in personal and business wireless technology, especially mobile communications. This phase is expected to reach maturity during 2005.

Ultimately, 3G is expected to include capabilities and features such as:

- Enhanced multimedia (voice, data, video, and remote control)
- Usability on all popular modes (cellular telephone, email, paging, fax, videoconferencing, and web browsing)
- Broad bandwidth and high speed (upwards of 2 Mbps)
- Routing flexibility (repeater, satellite, LAN)
- Operation at approximately 2 GHz transmit and receive frequencies
- Roaming capability throughout Europe, Japan, and North America

While 3G is generally considered applicable mainly to mobile wireless, it is also relevant to fixed wireless and portable wireless. The ultimate 3G system might be operational from any location on, or over, the earth’s surface, including use in homes, businesses, government offices and medical and military establishments. It can be used in personal and commercial land vehicles, private and commercial watercraft and marine craft, as well as private and commercial aircraft (except where passenger use restrictions apply). It can also be used by individuals (when they walk, for example) and even by spacecraft!

Proponents of 3G technology promise that it will “keep people connected at all times and in all places.” Researchers, engineers, and marketers are faced with the challenge of accurately predicting how much technology consumers will actually be willing to pay for. (Recent trends suggest that people sometimes prefer to be disconnected, especially when on holiday.)

Another concern involves privacy and security issues. As technology becomes more sophisticated and bandwidth increases, systems become increasingly vulnerable to attack by malicious hackers (known as crackers) unless countermeasures are implemented to protect against such activity.

Some UK network providers are already offering 3G services.

WWAN complementary technologies

GPS overview

The GPS (Global Positioning System) is a ‘constellation’ of 24 well-spaced satellites that orbit the Earth and make it possible for people with ground receivers to pinpoint their geographic location. The location accuracy is anywhere from 100 to 10 meters for most equipment. Accuracy can be pinpointed to within one meter with special military-approved equipment. GPS equipment is widely used in science and has now become sufficiently low-cost so that almost anyone can own a GPS receiver.

The GPS is owned and operated by the U.S. Department of Defense. However, it is available for general use around the world. Briefly, here’s how it works:

- 21 GPS satellites and three spare satellites are in orbit at 10,600 miles above the Earth. The satellites are spaced so that from any point on Earth, four satellites will be above the horizon.
- Each satellite contains a computer, an atomic clock and a radio. With an understanding of its own orbit and the clock, it continually broadcasts its changing position and time. (Once a day, each satellite checks its own sense of time and position with a ground station and makes any minor correction).
- On the ground, any GPS receiver contains a computer that ‘triangulates’ its own position by getting bearings from three of the four satellites. The result is provided in the form of a geographic position – longitude and latitude – to, for most receivers, within 10 meters.
- If the receiver is also equipped with a display screen that shows a map, the position can be shown on the map.
- If a fourth satellite can be received, the receiver/computer can figure out the altitude as well as the geographic position.
- If you are moving, your receiver may also be able to calculate your speed and direction of travel and give you estimated times of arrival to specified destinations.

The GPS is being used in science to provide data that has never been available before in the quantity and degree of accuracy that the GPS makes possible. Scientists are using the GPS to measure the movement of the arctic ice sheets, the Earth’s tectonic plates and volcanic activity.

GPS receivers are becoming consumer products. In addition to their outdoor use (hiking, cross-country skiing, ballooning, flying, and sailing), receivers can be used in cars to relate the driver’s location with traffic and weather information. GPS can be combined with GPRS to track the movement of vehicles or people.

spirit
DATA CAPTURE LTD

We hope that you have found this guide useful.

Spirit Data Capture Limited
www.spiritdatacapture.co.uk
Tel: +44 (0)870 166 2440
Email: info@spiritdatacapture.co.uk

If undelivered return to: Spirit Data Capture, Vale House, Aston Lane North, Preston Brook, Cheshire WA7 3PA