The *Bluetooth*™ Wireless Technology White Paper

is the registered trademark of Atmel Corporation,
2325 Orchard Parkway, San Jose, CA 95131

Rev. 1991A–11/00

Introduction

The *Bluetooth* wireless technology provides the means for the replacement of cables and infrared links that connect one device to another with a universal short-range radio link. Although this technology was initially developed for replacing cables, it has now evolved into a way to create small radio LANs.

The name *Bluetooth* comes from a Danish King, Harald Blaatand ("*Bluetooth*" in English) who lived from 940 to 981 and controlled Denmark and Norway.

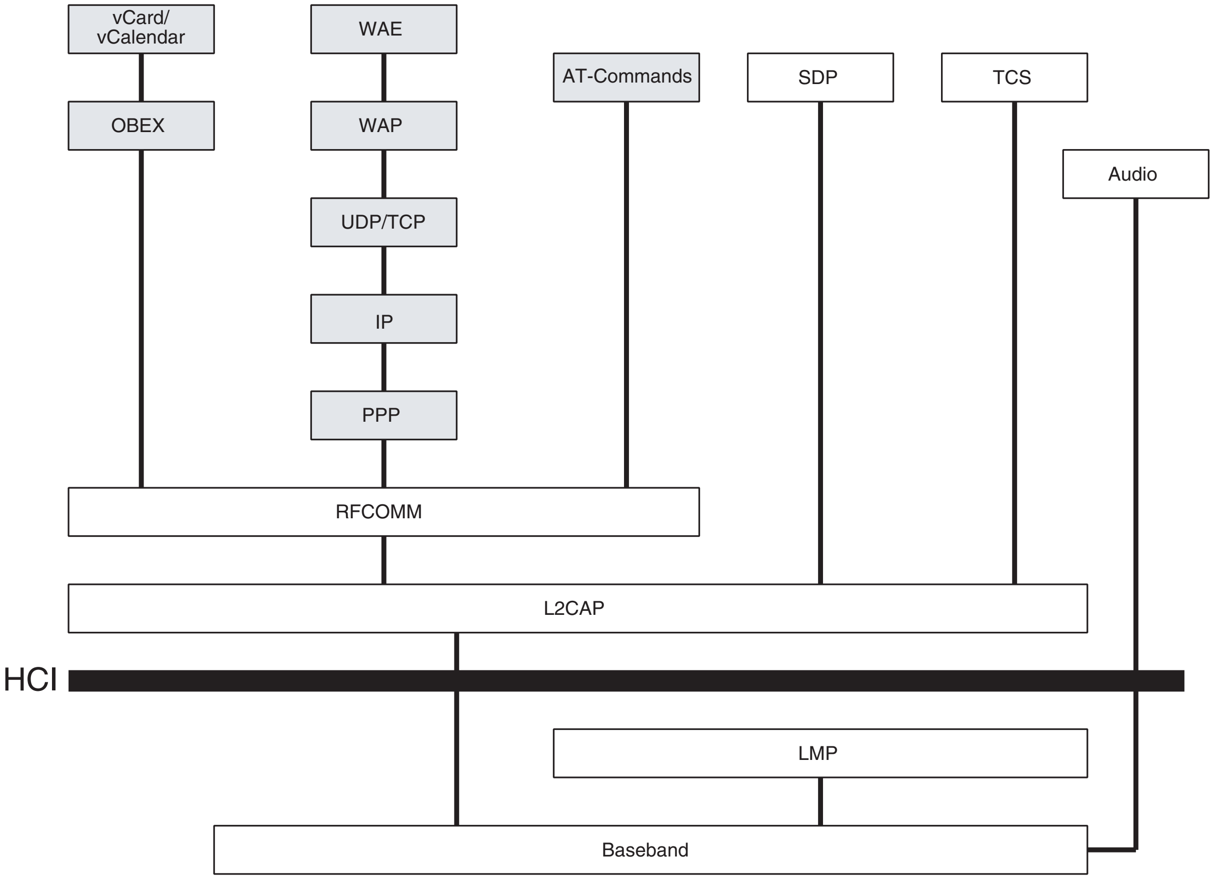
In February 1998, the *Bluetooth* Special Interest Group (SIG) was founded. At the start, it consisted of Ericsson Mobile Communications, Intel, IBM, Toshiba and Nokia Mobile Phones. This group represented the diverse market support that was needed to generate good support for the new technology. Today, more than 1,000 companies have joined the SIG to work for an open standard for the *Bluetooth* concept.

Bluetooth Architecture

The complete *Bluetooth* protocol stack is shown in Figure 1. Note that both *Bluetooth* specific protocols and non-*Bluetooth* specific protocols (shaded in Figure 1) comprise the protocol stack.

Protocols such as OBEX and UDP have been included in the protocol architecture to facilitate the adaptation of applications using such existing protocols. This gives for instance a number of existing applications supporting UDP an interface to the *Bluetooth* wireless technology.

Figure 1. The *Bluetooth* Protocol Stack



Bluetooth Specific Protocols

Baseband

The Baseband and Link Control Layer enables the physical RF link between *Bluetooth* units forming a piconet. This layer controls the *Bluetooth* unit's synchronization and transmission frequency hopping sequence. This layer also manages the two different link types defined in *Bluetooth*, Synchronous Connection Oriented (SCO) and Asynchronous Connectionless (ACL).

The ACL links, for data, and the SCO links, mainly for audio, can be multiplexed to use the same RF link.

Link Manager Protocol (LMP)

The LMP is responsible for link setup between *Bluetooth* units. It handles the control and negotiation of packet sizes used when transmitting data. The LMP also handles the management of power modes and power consumption. Finally, the LMP handles generation, exchange and control of link and encryption keys for authentication and encryption.

Host Controller Interface (HCI)

The HCI provides a uniform interface method for accessing the *Bluetooth* hardware capabilities. It contains a command interface to the Baseband controller and link manager and access to hardware status. Finally, it contains control and event registers.

Logical Link Control and Adaptation Protocol (L2CAP)

The L2CAP layer provides connection-oriented and connectionless data services to upper layers.

The L2CAP performs the following tasks:

- Multiplexing – L2CAP must support protocol multiplexing since a number of protocols (e.g., SDP, RFCOMM and TCS Binary) can operate over L2CAP.
- Segmentation and Reassembly – L2CAP performs segmentation and reassembly for data packets which exceed the Maximum Transmission Unit (MTU). These packets must be segmented before transmitted. The reverse functionality must be performed at the receiver's end.
- Quality of Service – The exchange of information regarding current Quality of Service for the connection between two *Bluetooth* units can take place after the establishment of an L2CAP connection.
- Groups – The L2CAP supports a group abstraction that permits implementations for mapping groups on to a piconet.

RFCOMM

The RFCOMM protocol is a serial port emulation protocol that covers applications that make use of the serial ports of the unit. RFCOMM emulates RS-232 control and data signals over the *Bluetooth* baseband. It provides transport capabilities for upper level services (e.g. OBEX) that use a serial line as the transport mechanism.

Service Discovery Protocol (SDP)

The SDP defines how a *Bluetooth* client's application shall act to discover available *Bluetooth* servers' services. It defines how a client can search for a service without knowing anything of the available services. The SDP provides means for the discovery of new services becoming available when the client enters an area where a *Bluetooth* server is operating. It also provides the means to detect when a service is no longer available.

Telephony Control – Binary (TCS Binary)

The TCS Binary is a bit-oriented protocol, which defines the call control signaling for the establishment and release of speech and data calls between *Bluetooth* units. Furthermore, it provides functionality to exchange signaling information unrelated to ongoing calls.

Audio

The *Bluetooth* specification enables audio transmissions between one or more *Bluetooth* units. Audio data do not go through the L2CAP layer, but go directly, after opening a *Bluetooth* link and a straightforward setup, between two *Bluetooth* units.

Specific Protocols without *Bluetooth*

Telephony Control – AT Commands

Bluetooth supports a number of AT commands for transmitting control signals for telephony control through the serial port emulation (RFCOMM).

Point-to-Point Protocol (PPP)

The PPP is a packet-oriented protocol and must therefore use its serial mechanisms to convert the packet data stream into a serial data stream. It runs over RFCOMM to accomplish point-to-point connections.

UDP/TCP – IP Protocols

The UDP/TCP and IP standards allow *Bluetooth* units to communicate with other units connected, for instance, to the Internet. Therefore, the *Bluetooth* unit can act as a bridge to the Internet. The TCP/IP/PPP protocol configuration is used for all Internet Bridge usage scenarios in *Bluetooth* 1.0 and OBEX in future versions. The UDP/IP/PPP configuration is available as a transport to WAP.

Wireless Application Protocol (WAP)

The WAP is a wireless protocol specification that works across a variety of wide-area wireless network technologies bringing the Internet to mobile devices. *Bluetooth* can be used like other wireless networks with regard to WAP to provide a bearer for transporting data between the WAP client and its adjacent WAP server.

Furthermore, *Bluetooth*'s ad hoc networking capability gives a WAP client unique possibilities regarding mobility compared with other WAP bearers.

Also, the server push capability of the WAP technology opens new possibilities for distributing information to handheld devices on location basis, if used over *Bluetooth*. For example, shops can push special price offers to a WAP client when it comes within *Bluetooth* range.

OBEX Protocol

OBEX is an optional application layer protocol designed to enable units supporting infrared communication to exchange a wide variety of data and commands. It uses a client-server model and is independent of the transport mechanism and transport API. OBEX uses RFCOMM as the main transport layer.

Bluetooth Radio Parameters

Bluetooth units operate on the ISM band, at 2.45 GHz. The transmitting power is between 1 and 100 mW. The low power consumption implies that a *Bluetooth* unit can operate on the power from a small battery for a long time. These hardware characteristics make it possible to fit a *Bluetooth* unit in many electrical devices. The maximum *Bluetooth* range is 10 m, with a possibility to extend it to 100 m.

The maximum bit rate is 1 Mbps. However, the maximum effective payload is lower because the different protocol layers require data payload for signaling to their corresponding layers in the unit with which the device is communicating. Estimates have indicated data transfer rates up to 720 kbps. All piconets share the 80 MHz band, where each piconet uses 1 MHz, thus, as long as the piconets pick different hop sequences, no sharing of 1 MHz hop channels occurs.

Bluetooth and Frequency Hopping

In *Bluetooth* interference is avoided by using a frequency-hopping (FH) spread spectrum technology. FH is a technology well suited for low-power, low-cost radio implementations and is used in some wireless LAN (WLAN) products. The *Bluetooth* specification defines a high hop rate of 1600 hops per second instead of just a few hops per second used in other implementations.

The frequency band is divided into a number of hop channels with every channel being just a fraction of the total frequency band. In *Bluetooth* every channel is used for 625 µs (one slot) followed by a hop in a pseudo-random order to another channel for another 625 µs transmission repeated constantly. That way the *Bluetooth* traffic is spread over the entire ISM band and a very good interference protection is achieved. If one of the transmissions is jammed, the probability of interference on the next hop channel is very low. Furthermore, error correction algorithms are used to correct the fault caused by jammed transmissions.

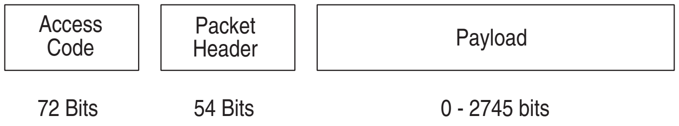
The 79 hop carriers have been defined for the *Bluetooth* wireless technology except for Japan, France and Spain where 23 hop carriers have been defined, because the ISM-band is narrower there.

When *Bluetooth* units are communicating, one unit acts as master and the rest act as slaves. The master's unit system clock and the master identity are the central parts in the frequency hopping technology. The hop channel is determined by the hop sequence and by the phase in this sequence. The identity of the master determines the sequence and the master unit's system clock determines the phase. In the slave unit, an offset may be added to its system clock to create a copy of the master's clock. In this way every unit in the *Bluetooth* connection holds synchronized clocks and the master identity, that uniquely identifies the connection.

Packet Format

The *Bluetooth* packets have a fixed format (Figure 2). A 72-bit access code comes first in the packet. The access code is based on the master's identity and the master's system clock, for example, it provides the means for synchronization. This code is unique for the channel and used by all packets transmitting on a specific channel. The 54-bit header following the access code contains error correction, retransmission and flow control information. The error correction information can be used for correcting faults in the payload and in the header itself. Finally, the payload field can be up to 2,745 bits.

Figure 2. The *Bluetooth* Packet Format



Piconet and Scatternet

Any two *Bluetooth* devices that come within range of each other can set up an ad-hoc connection, which is called a piconet. Every piconet consists of up to eight units. There is always a master unit in a piconet and the rest of the units act as slaves. The unit that establishes the piconet becomes the master unit. The master unit can change later but there can never be more than one master.

Several piconets can exist in the same area. This is called scatternet. Within one scatternet all units share the same frequency range, but each piconet uses different hop sequences and transmits on different 1 MHz hop channels. All piconets share the 80 MHz band, thus, as long as the piconets pick different hop frequencies, no sharing of hop channels occurs.

Link Types

The *Bluetooth* specification defines two link types, Asynchronous Connectionless (ACL) and Synchronous Connection Oriented (SCO). Different master-slave pairs in the same piconet can use different link types. The link type may be changed during a session.

The SCO links are primarily used for voice traffic and their data rate is 64 kbps.

ACL links are used mainly for data traffic and support broadcast messages (i.e. from the master to all slaves to the piconet). Multi-slot packets use the ACL link type and can reach the maximum data rate of 721 kbps in one direction and 57.6 kbps in the other direction if no error correction is used.

Security

Authentication is used in *Bluetooth* to prevent unwanted access to data and to prevent falsifying the message originator. Encryption is used to prevent eavesdropping. These two techniques combined with the frequency hopping technique and the limited transmission range for a *Bluetooth* unit (usually 10 m) give the technology higher protection against eavesdropping.

Three modes of security are defined in *Bluetooth*. The need for a particular mode is dependent on what kind of application is executed.

- Non-secure mode – No authentication or encryption is used.
- Service-level security mode – Security procedures are initiated after L2CAP channel establishment. This security mode provides the possibility to define trust levels for the services and units used respectively.
- Link-level security mode – Security procedures are initiated before the link setup at the LMP level is completed. This mode is based on the use of link keys that are secret 128-bit random numbers stored individually for each pair of devices in a *Bluetooth* connection. Each time two *Bluetooth* units communicate, the link key is used for authentication and encryption.

Basic *Bluetooth* Profiles

To avoid different interpretations of the *Bluetooth* standard regarding how a specific type of application should be mapped to *Bluetooth*, the SIG has defined a number of user models and protocol profiles.

A profile defines a selection of messages and procedures from the *Bluetooth* specifications and gives an unambiguous description of the air interface for specified services and use cases. A profile can be described as a vertical slice through the protocol stack. It defines options in each protocol that are mandatory for the profile. It also defines parameter ranges for each protocol.

There are four general profiles defined, on which some of the highest prioritized user models and their profiles are directly based on. These four models are the Generic Access Profile (GAP), the Service Discovery Application Profile (SDAP), the Serial Port Profile and the Generic Object Exchange Profile (GOEP).

Generic Access Profile (GAP)

The Generic Access Profile defines how to *Bluetooth* units discover and establish a connection with each other. GAP handles discovery and establishment between units that are unconnected and ensures that any two *Bluetooth* units, regardless of manufacturer and application, can exchange information via *Bluetooth* to discover what type of applications the units support.

Bluetooth units must conform to GAP to ensure basic interoperability and coexistence.

Service Discovery Application Profile (SDAP)

It is expected that the number of services that can be provided over *Bluetooth* links will increase in an undetermined (and possibly uncontrolled) manner. Therefore, procedures need to be established to aid a user of a device enabled with *Bluetooth* to sort the ever-increasing variety of services that will become available to him/her. While many of the services enabled with *Bluetooth* that may be encountered are currently unknown, a standardized procedure can still be put into place on how to locate and identify them.

The *Bluetooth* protocol stack contains a Service Discovery Protocol (SDP) that is used to locate services that are available on or via devices in the vicinity of a device enabled with *Bluetooth*. Having located what services are available in a device, a user may then select to use one or more of them. Even though SDP is not directly involved in accessing services, information retrieved via SDP facilitates service access by using it to properly condition the local *Bluetooth* stack to access the desired service.

The Service Discovery Application Profile (SDAP) defines the protocols and procedures that shall be used by a service discovery application on a device to locate services in other devices enabled with *Bluetooth* using the SDP. With regard to this profile, the service discovery application is a specific user-initiated application.

The SDAP is dependent on the GAP (i.e. SDAP re-uses parts of the GAP).

Serial Port Profile

The Serial Port Profile defines how to set up virtual serial ports on two devices and connecting these with *Bluetooth*. Using this profile provides the *Bluetooth* units with an emulation of a serial cable using RS232 control signaling (RS232 is a common interface standard for data communications equipment). The profile ensures that data rates up to 128 Kbps can be used.

The Serial Port Profile is dependent on the GAP.

Generic Object Exchange Profile (GOEP)

The Generic Object Exchange profile defines the protocols and procedures that shall be used by the applications providing the usage models which need the object exchange capabilities. The usage model can be, for example, Synchronization, File Transfer, or Object Push model. The most common devices using these usage models can be notebook PCs, PDAs, smart phones and mobile phones.

The GOEP is dependent on the Serial Port Profile.

Other *Bluetooth* Profiles and Usage Models

Cordless Telephony Profile

The Cordless Telephony profile defines the protocols and procedures that shall be used by devices implementing the use case called “3-in-1 phone”.

The “3-in-1 phone” is a solution for providing an extra mode of operation to cellular phones, using *Bluetooth* as a short-range bearer for accessing fixed network telephony services via a base station. However, the “3-in-1 phone” use case can also be applied generally for wireless telephony in a residential or small office environment, for example for cordless-only telephony or cordless telephony services in a PC – hence the profile name “Cordless Telephony”.

This use case includes making calls via the base station, making direct intercom calls between two terminals and accessing supplementary services provided by the external network.

Intercom Profile

The Intercom profile defines the protocols and procedures that shall be used by devices implementing the intercom part of the usage model called “3-in-1 phone”. More popularly, this is often referred to as the “walkie-talkie” usage of *Bluetooth*.

Headset Profile

The Headset profile defines the protocols and procedures that shall be used by devices implementing the usage model called “Ultimate Headset”. The most common examples of such devices are headsets, personal computers and cellular phones.

The headset can be wireless connected for the purposes of acting as the device’s audio input and output mechanism, providing full duplex audio. The headset increases the user’s mobility while maintaining call privacy.

Dial-up Networking Profile

The Dial-up Networking Profile defines the protocols and procedures that shall be used by devices implementing the usage model called “Internet Bridge”. The most common examples of such devices are modems and cellular phones.

The scenarios covered by this profile are the following:

- Usage of a cellular phone or modem by a computer as a wireless modem for connecting to a dial-up Internet access server, or using other dial-up services
- Usage of a cellular phone or modem by a computer to receive data calls

Fax Profile

The Fax profile defines the protocols and procedures that shall be used by devices implementing the fax part of the usage model called “Data Access Points, Wide Area Networks’ (see *Bluetooth* SIG MRD).

A *Bluetooth* cellular phone or modem may be used by a computer as a wireless fax modem to send or receive a fax message.

LAN Access Profile

This profile defines LAN Access using PPP over RFCOMM. There may be other means of LAN Access in the future.

PPP is a widely deployed means of allowing access to networks. PPP provides authentication, encryption, data compression and multi-protocol facilities. PPP over RFCOMM has been chosen as a means of providing LAN Access for *Bluetooth* devices because of the large installed base of devices equipped with PPP software.

This profile does not deal with conferencing, LAN emulation, ad hoc networking or any other means of providing LAN Access. These functions are, or may be, dealt with in other *Bluetooth* profiles.

The LAN Access profile defines how PPP networking is supported in the following situations:

- LAN Access for a single *Bluetooth* device.
- LAN Access for multiple *Bluetooth* devices.
- PC-to-PC (using PPP networking over serial cable emulation).

Object Exchange Profile

The Object Push profile defines the requirements for the protocols and procedures that shall be used by the applications providing the Object Push usage model. This profile makes use of the Generic Object Exchange profile (GOEP) to define the interoperability requirements for the protocols needed by applications. The most common devices using these usage models can be notebook PCs, PDAs and mobile phones.

The scenarios covered by this profile are the following:

- Usage of a *Bluetooth* device (e.g. a mobile phone to push an object to the inbox of another *Bluetooth* device). The object can, for example, be a business card or an appointment.
- Usage of a *Bluetooth* device (e.g., a mobile phone to pull a business card from another *Bluetooth* device).
- Usage of a *Bluetooth* device (e.g., a mobile phone to exchange business cards with another *Bluetooth* device). Exchange defined as a push of a business card followed by a pull of a business card.

File Transfer Profile

The File Transfer profile defines the requirements for the protocols and procedures that shall be used by the applications providing the File Transfer usage model. This profile uses the Generic Object Exchange profile (GOEP) as a base profile to define the interoperability requirements for the protocols needed by the applications. The most common devices using these usage models can be (but are not limited to) PCs, notebooks and PDAs.

The scenarios covered by this profile are the following:

- Usage of a *Bluetooth* device (e.g., a notebook PC) to browse an object store (file system) of another *Bluetooth* device. Browsing involves viewing objects (files and folders) and navigating the folder hierarchy of another *Bluetooth* device. For example, one PC browsing the file system of another PC.
- A second usage is to transfer objects (files and folders) between two *Bluetooth* devices. For example, copying files from one PC to another PC.
- A third usage is for a *Bluetooth* device to manipulate objects (files and folders) on another *Bluetooth* device. This includes deleting objects and creating new folders.

Synchronization Profile

The Synchronization profile defines the requirements for the protocols and procedures that shall be used by the applications providing the Synchronization usage model. This profile makes use of the Generic Object Exchange profile (GOEP) to define the interoperability requirements for the protocols needed by applications. The most common devices using these usage models might be notebook PCs, PDAs and mobile phones.

The scenarios covered by this profile are:

- Usage of a mobile phone or PDA by a computer to exchange PIM (Personal Information Management) data, including a necessary log information to ensure that the data contained within their respective Object Stores is made identical. Types of the PIM data are, for example, phonebook and calendar items.
- Use of a computer by a mobile phone or PDA to initiate the previous scenario (Sync Command Feature).
- Use of a mobile phone or PDA by a computer to automatically start synchronization when a mobile phone or PDA enters the RF proximity of the computer.

Competing Technologies

There are a number of technologies competing with *Bluetooth* wireless technologies including IrDA, IEEE 802.11, UWB and Home RF.

The IrDA is an infrared interface standard with main disadvantages: its limitation to point-to-point connections (only two parties in a connection), its need for line of sight (since it is based on infrared light) and the existence of numerous incompatible implementations.

The IEEE 802.11 standard is the main competitor of the *Bluetooth* wireless technology in the WLAN market segment. The main differences between the two standards are:

- IEEE 802.11 has higher transmission capacity.
- The number of simultaneous users is higher for IEEE 802.11-based systems
- The *Bluetooth* hardware size is considerably smaller.
- The *Bluetooth* unit is considerably cheaper.
- The number of frequency hops is considerably higher in *Bluetooth*.

Ultra-wideband Radio (UWB) technology is based on short pulses which are transmitted in a broad frequency range. The technique is not fully developed yet but might be a threat to *Bluetooth* since it is superior in capacity and power consumption. The UWB prototypes indicate payloads up to 1.25 Mbps with 70 m range at just 0.5 mW power consumption.

Home RF is a technique developed for the home market. It is based on the DECT concept and operates in the 2.4 GHz frequency band. It has many similarities with *Bluetooth* (pricing, range, transmitting power, etc.). The major differences are that Home RF can handle up to 127 units per net while *Bluetooth* handles 8 units per piconet and that Home RF uses just 50 frequency hops per second while *Bluetooth* uses 1,600.

Bluetooth offers several benefits compared with its competitors including the small hardware dimensions, low pricing and low power consumption. Furthermore, there is no obvious single competitor in all the market segments in which the *Bluetooth* wireless technology can operate.

The advantages make it possible to introduce support for *Bluetooth* in many types of devices at a low price. The diversity in product offerings (notebooks, mobile phones, PDAs, computers, hardware) from companies in the *Bluetooth* SIG and their broad support for the technique creates a unique market position.

References

1. Specification of the *Bluetooth* System Vol. 1 – Core, v1.0 B, December 1, 1999.
2. Specification of the *Bluetooth* System Vol. 2 – Profiles, v1.0 B, December 1, 1999.
3. *Bluetooth* White Paper, AU-System, October 1999.
4. *Bluetooth* Overview, www.*bluetooth*.com.

Atmel Headquarters

Corporate Headquarters
2325 Orchard Parkway
San Jose, CA 95131
TEL (408) 441-0311
FAX (408) 487-2600

Europe
Atmel SarL
Route des Arsenaux 41
Casa Postale 80
CH-1705 Fribourg
Switzerland
TEL (41) 26-426-5555
FAX (41) 26-426-5500

Asia
Atmel Asia, Ltd.
Room 1219
Chinachem Golden Plaza
77 Mody Road Tsimhatsui
East Kowloon
Hong Kong
TEL (852) 2721-9778
FAX (852) 2722-1369

Japan
Atmel Japan K.K.
9F, Tonetsu Shinkawa Bldg.
1-24-8 Shinkawa
Chuo-ku, Tokyo 104-0033
Japan
TEL (81) 3-3523-3551
FAX (81) 3-3523-7581

Atmel Operations

Atmel Colorado Springs
1150 E. Cheyenne Mtn. Blvd.
Colorado Springs, CO 80906
TEL (719) 576-3300
FAX (719) 540-1759

Atmel Rousset
Zone Industrielle
13106 Rousset Cedex
France
TEL (33) 4-4253-6000
FAX (33) 4-4253-6001

Atmel Smart Card ICs
Scottish Enterprise Technology Park
East Kilbride, Scotland G75 0QR
TEL (44) 1355-803-000
FAX (44) 1355-242-743

Atmel Grenoble
Avenue de Rochepleine
BP 123
38521 Saint-Egreve Cedex
France
TEL (33) 4-7658-3000
FAX (33) 4-7658-3480

Fax-on-Demand
North America:
1-(800) 292-8635
International:
1-(408) 441-0732

e-mail
literature@atmel.com

Web Site
http://www.atmel.com

BBS
1-(408) 436-4309

Atmel Corporation makes no warranty for the use of its products, other than those expressly contained in the Company's standard warranty which is detailed in Atmel's Terms and Conditions located on the Company's web site. The Company assumes no responsibility for any errors which may appear in this document, reserves the right to change devices or specifications detailed herein at any time without notice, and does not make any commitment to update the information contained herein. No licenses to patents or other intellectual property of Atmel are granted by the Company in connection with the sale of Atmel products, expressly or by implication. Atmel's products are not authorized for use as critical components in life support devices or systems.

Printed on recycled paper.

1991A–11/00/xM