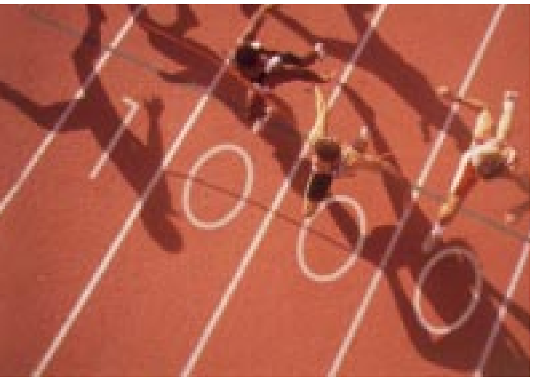
Bluetooth
SIGnal
The official newsletter of the Bluetooth Special Interest Group

Issue no.2, September 1999

Bluetooth™



Over 1000 Bluetooth SIG members in less than 18 months!

Welcome to the second edition of the Bluetooth™ SIGnal. To our amazement, the Bluetooth Special Interest Group (SIG) now comprises more than 1000 members. This has exceeded everyone's wildest expectations, especially in the short time – less than 18 months – since the SIG was formed. An interview with the 1000th member of the Bluetooth SIG is presented below. We now look forward to the 2000th member! Who knows, it may even coincide with the new millennium.

The Bluetooth Specification Release 1.0 has now been available for a couple of months. Such a massive document is bound to contain a number of errors on introduction, but judging from the minimal feedback received so far, the technical editors must have done a very solid job. Perhaps after the few months it will take to read though and fully understand the specification, we will receive more feedback – time will tell.

Measures to ensure quality

When the specification was released, an important section was missing, the one covering the qualification of early products. Because of the extensive work involved in creating the test equipment and test specifications, the full qualification program will not be in place until next year. To ensure interoperability between early Bluetooth-enabled products, the SIG has decided to include profile testing in the early qualification program. This will delay the program until the end of this year. Consequently, no Bluetooth-enabled products can realistically be shipped until early next year. We believe this is a wise decision to ensure that early products will also meet the high quality demands on Bluetooth-enabled devices.

A new figure mark soon

Our pleasure at the rapidly increasing Bluetooth SIG membership has been dampened somewhat by a problem related to the figure mark (based on a Viking ship sail and elliptical radio waves) in the Bluetooth trademark. Unknown to us, another company (visit http://www.vnu.com) had filed a registration for a similar figure mark to ours in Europe a few weeks before we did. Because of the short time span between the two filings, the similarity was not discovered in the legal search.

The result is that, to avoid any legal obstacles, the Bluetooth SIG is now working on a permanent solution to the Bluetooth figure mark. In the meantime, only the word mark Bluetooth™ must be used in all marketing material, with or without the tagline "Wireless Connections Made Easy." Further details regarding the use of the Bluetooth trademark will be found in the Bluetooth Brand Book now being revised.

Several exciting events

We look forward to a hectic yet stimulating fall with a number of interesting Bluetooth events, such as the first exhibition with a separate Bluetooth pavilion, Comdex in Las Vegas during November 15–19. Other events include the first Bluetooth-endorsed conference* in Amsterdam on November 8–10, and, of course, the huge and exciting Bluetooth Developers Conference in Los Angeles between December 6–9.

We hope to see many of you there.

Anders Edlund,
Marketing Director, Bluetooth
Ericsson Mobile Communications AB.

* A Bluetooth-endorsed conference is allowed to use the Bluetooth brand elements, but the content of the conference is not controlled in any way by the Bluetooth SIG even though SIG speakers usually take part.

Meet Unipower, the 1000th SIG member!

At the end of August, Unipower became the 1000th Bluetooth SIG member. We thought that we would highlight this remarkable event by interviewing the Managing Director of Unipower, Hugo Patten.

Q. Who is Unipower?

Unipower Systems is a software and services company based in the UK (London and St. Albans), France (Paris) and the USA (New Jersey). It focuses on deploying innovative Electronic Commerce and Knowledge Management solutions. The company offers independent strategic IT consultancy as well as extensive expertise in database integration and application development.

Unipower's Magic suite of applications delivers the world's most powerful e-commerce environments for both business-to-business and business-to-consumer markets. We work with a number of partners, who support the implementation and integration of eBusiness. Amongst them are Cap Gemini, Logica, Symbol Technologies, TMS, BT and many others. You can read more about us at http://www.unipower.net

Q. How does it feel to be the 1000th Bluetooth SIG member?

Well, firstly it feels reassuring that such a large following of key companies is ratifying the Bluetooth technology. Secondly it gives Unipower an opportunity to both enhance its product development offerings, and hopefully add value to the whole partnership in terms of creating applications people can relate to.

Q. What are your personal views of the Bluetooth technology?

The ideal of having a set of evolving standards to work with in this field is a key element in continuous development. We, the software and hardware vendors, must pool our abilities to create a seamless environment that 'real' people will want to make use of in their homes and offices.

Q. Have you been closely following the development of the Bluetooth technology?

Unipower has a vested interest in all devices and communication methods that can be placed in homes or mobile environments, be it set-top boxes, mobile phones, or Bluetooth-enabled devices. So, yes, Unipower has been following the project very closely. Obviously the buy-in from the major vendors and the cost base forms the key to giving the whole technology a competitive edge.

Q. What do you regard as its biggest advantages?

I would say cost, it's a *de facto* standard, it's flexible, it provides a coherent design, and of course its very portable.

> "The technology is well founded, cost effective, and could revolutionize the way we live."

Q. How do you intend to apply the Bluetooth technology in your business activities and what will you concentrate on?

The Bluetooth technology will allow us to offer home and mobile devices that enable free use of seamless technology involving e-commerce and Knowledge Management systems. We want to be able to offer the same level of e-commerce applications in terms of ease of use that, for example, banking standing orders and direct debits do. We hope that this way of facilitating the purchase of day-to-day goods will reduce the time spent on tedious chores!

We already have a prototype, in the form of a home shopping application, working on the next generation of mobile phones. This enables the user to add extra items to an order, whether on a train or in an office, and also to check the expected delivery time. We see the Bluetooth approach as a technology that will extend that kind of flexibility.

Hugo Patten, Managing Director of Unipower.

Q. Did you consider alternative communication technologies before deciding on the Bluetooth radio?

Unipower has worked on a number of different communication technologies. However, in terms of the type of environments that the Bluetooth technology is targeting, we consider it the only non-proprietary method of achieving this at scale and at low cost.

Q. What took you so long to become a Bluetooth SIG member?!

As we like to take an active part in all of the technology areas we subscribe to, we simply had too many clients wanting systems implemented at the same time. One could say that we had a limited bandwidth for so many leading-edge developments.

Q. What was the deciding factor?

Belief in the technology, and the need to create e-commerce systems that use real 'metaphors' that people understand, rather than the keyboard, which is already hundreds of years old.

Q. Do you think the Bluetooth technology has a bright future?

Based on the number of adopters, I think that Bluetooth communication will succeed. The technology is well founded, cost effective, and could revolutionize the way we live. That is the goal for Bluetooth applications, and it's up to everyone involved to create the solutions for living based on this technology.

Wireless Personal Area Networks

Imagine living your entire life within the confines of a bubble. Now imagine that this bubble has a radius of 10 meters. This invariable bubble is called your Personal Operating Space (POS). Now look around in your bubble. How many electronic devices do you see? How many wires do you see? The Bluetooth technology provides wireless connectivity among these devices within (or moving into) your POS. These wirelessly connected devices create a network called a Wireless Personal Area Network (WPAN). In the Wide Area Network (WAN), Metropolitan Area Network (MAN), and Local Area Network (LAN) hierarchy, the WPAN's scope is the smallest and least developed.

In March of 1998, the WPAN Study Group was formed. The study group's goal was to investigate the need for a wireless network standard for devices within a POS. In May of 1998, the Bluetooth Special Interest Group (SIG) was formed. In March of 1999, the WPAN study group became IEEE 802.15, the WPAN Working Group. The working group's goal is to define a wireless communications standard for a PAN, focusing on low power consumption, small size, and low cost. In July of 1999, the Bluetooth SIG released the Bluetooth 1.0 Specification.

WPAN of the Future

The obvious applications of a WPAN are in the office workspace. With the Bluetooth technology, your essential workspace electronic devices will be wirelessly networked together. These could include your desktop, mobile computer, printer, handheld device, mobile phone, pager, portable stereo, etc. Imagine wirelessly checking e-mail in an airport by connecting to data access points or wirelessly printing documents from the printer in the back of the plane. The less obvious applications of a WPAN are outside of the office. Imagine an oven that sends a message to the TV you are watching when your meat loaf is done, or a handgun that only fires when an authorized person uses it.

In today's environment, information is our most valuable commodity. In an electronic future with smaller, cheaper, and more powerful devices, the speed and convenience at which information is accessible will be exponentially more important. By creating a WPAN of these devices, the Bluetooth technology enables a future where a lifetime of knowledge may be accessed through gateways worn on the body.

For more information about WPANs, go to http://grouper.ieee.org/groups/802/15/

Bluetooth Service Discovery and Related Technologies

As computing continues to move to a network-centric model, finding and making use of services that may be available in the network becomes increasingly important. Services can include common ones such as printing, paging and faxing, as well as various kinds of information access like teleconferencing, network bridges and access points and e-commerce facilities – most any kind of service that a server or service provider might offer.

In addition to the need for a standard way of discovering available services, there are other considerations. For instance, getting access to the services (finding and obtaining the protocols, access methods, "drivers" and other code necessary to utilize the service), controlling access to the services, advertising the services, choosing among competing services, billing for services, and so on. This problem is widely recognized; many companies, standards bodies and consortia are addressing it at various levels in various ways. Service Location Protocol (SLP) [1], Jini™ [2], Universal Plug and Play™ (UPnP™) [3] and Salutation™ [4], to name just a few, all address some aspect of service discovery.

A dedicated protocol

The Bluetooth Service Discovery Protocol (SDP) addresses service discovery specifically for the Bluetooth environment. It is optimized for the highly dynamic nature of Bluetooth communications. SDP focuses primarily on discovering services available from or through Bluetooth-enabled devices. SDP does not define methods for accessing services; once services are discovered with SDP, they can be accessed in various ways, depending upon the service. This might include the use of other service discovery and access mechanisms such as those mentioned above.

SDP provides a means for other protocols to be used along with SDP in those environments where this can be beneficial. For example, using SDP, a client could discover a service offered by a Bluetooth-enabled device. One attribute of that service might specify that the service supports Salutation, and Salutation

>> STORY CONTINUES >>

>> STORY CONTINUES >>

could then be used for further interaction with that service. (The Bluetooth SIG has published a white paper describing mapping between Salutation and SDP, see [5]; mappings to other protocols may be published in the future). Although SDP can coexist with other service discovery protocols, it does not require them. In Bluetooth environments, services can be discovered using SDP and can be accessed using other protocols defined by the Bluetooth SIG or by others.

Why develop another?

With so many available service discovery protocols to choose from, why has the Bluetooth SIG specified its own service discovery protocol? As noted above, the dynamic nature of Bluetooth communications calls for a simple and compact service discovery protocol. As a contributing adopter member of the Bluetooth SIG, Motorola® proposed a protocol based upon their Piano™ [6] platform, a technology suited to wireless mobile applications such as found in Bluetooth environments. The SIG adopted this proposal and made many modifications and adaptations to produce the Bluetooth Service Discovery Protocol found in the Bluetooth Specification Release 1.0. With this specification release, the SIG provides service discovery that is well-suited to Bluetooth environments, is integrated into the Bluetooth software stack, and can coexist with many other service discovery protocols and technologies.

(The trademarks given in the above article are the property of their respective owners.)

References

[1] IETF RFC 2165,
http://www.ietf.org/rfc/rfc2165.txt

[2] http://java.sun.com/jini

[3] http://www.upnp.org

[4] http://www.salutation.org

[5] Mapping Salutation Architecture APIs to Bluetooth Service Discovery Layer, http://www.bluetooth.com/document/download.asp?doc=172

[6] http://www.mot.com/GSS/SSTG/piano/

Other resources

Bluetooth Specification Release 1.0,
Service Discovery Protocol,
http://www. bluetooth.com

Bluetooth Profiles Release 1.0, Service
Discovery Application Profile,
http://www.bluetooth.com

Discovering Devices and Services in Home Networks, an IBM white paper, http://www-3.ibm.com/pvc/nethome/networking.html

Putting it simply

Bluetooth communication security

As radio signals can be easily intercepted, it is important that Bluetooth-enabled devices have built-in security to prevent eavesdropping or falsifying the origin of messages (spoofing). The following link-level security features of the Bluetooth technology achieve these basic objectives:

- *Authentication*, which prevents spoofing and unwanted access to critical data and functions.
- *Encryption*, which prevents eavesdropping and maintains link privacy.

In addition to these link-level functions, frequency hopping (described in Bluetooth SIGnal 1 available on the official Bluetooth website) and the limited transmission range of Bluetooth-enabled devices – usually about 10 m – also help to prevent eavesdropping.

Due to the fact that applications and devices will have different demands on data security, flexibility in the use of the link-level security is needed. The Bluetooth Specification [1] defines three security modes that cover the functionality and application of the device:

Mode 1. Non-secure.
Mode 1 is used with devices having no critical applications. It bypasses the link-level security functions and is suitable for accessing, e.g., databases containing non-sensitive information. The automatic exchange of business cards is a typical example of non-secure data transfer.

Mode 2. Service-level security.
This mode allows versatile access procedures, especially for running applications with different security requirements in parallel. A more detailed description is given below, and a white paper is available describing this mode [2].

Mode 3. Link-level security.
In this mode the link manager enforces security at a common level for all applications at the very beginning of the connection. Although less flexible, this mode is well suited to enforcing a common security level, and it is easier to implement than mode 2.

Link-level security

All link-level security functions are based on the concept of link keys. A secret link key is a 128 bit random number stored individually for each pair of devices. Each time these two devices communicate via Bluetooth transceivers, the link key is used for authentication and encryption, without any influence of the piconet topology (see Figure 1). The most secure type of link key is a combination key, derived from the input of both devices. For devices with low storage capabilities, there is also the option of choosing a unit key, which may be used for several remote devices. Additionally, for broadcasting, a temporary key is needed, which naturally cannot be used for authentication but

>> STORY CONTINUES >>

>> STORY CONTINUES >>

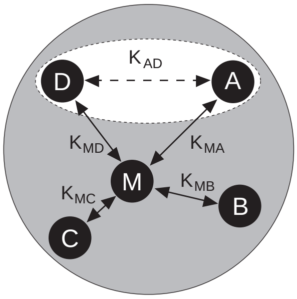


Figure 1. Link keys (K) are required for authentication and encryption between Bluetooth-enabled devices. This piconet comprises a master device (M) and four slave devices (A-D).

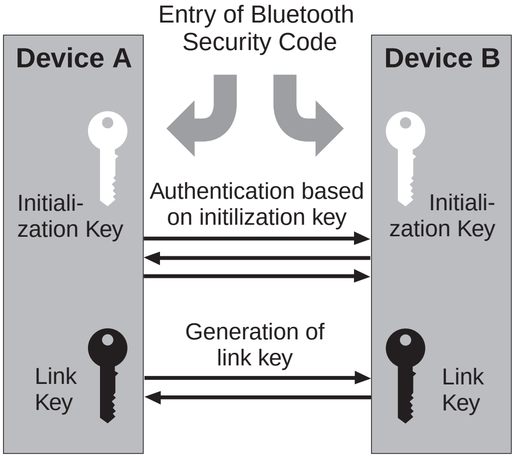


Figure 2. The first-time pairing process.

prevents eavesdropping from outside the piconet (but not from members sharing this temporary key).

Authentication requires no user input. It involves a device-to-device challenge and response scheme that requires a 128-bit common secret link key, a 128-bit challenge and a 32-bit response.

For the first time only that two devices communicate, an initialization procedure is needed to create a common link key in a safe manner. This procedure is called pairing (see Figure 2). The standard way of doing this assumes that the user has access to both devices at the same time. For first-time connection, pairing requires the user to key in a Bluetooth security code of up to 16 bytes or 128 bits into paired devices. However, when this is done manually, this code will usually be shorter.

Although the Bluetooth security code is often referred to as a “PIN” (Personal Identity Number), it is not a code the user has to keep secret or memorize, as it is only used once. When for some reason a link key is deleted and the initial pairing must be repeated, any Bluetooth security code can be entered by the user again. In the case of low security requirements, it is possible to have a fixed code in devices having no man-machine interface to allow pairing.

The pairing procedures involves:

a) Generation of a common random number initialization key from the user-entered Bluetooth security code in paired devices. This is used once and then discarded.

b) Authentication which checks that the Bluetooth security code is identical in the paired devices.

c) Generation of a common 128-bit random number link key – stored temporarily or semi-permanently in paired devices.

As long as this current link key is stored in both devices, no repetition of pairing is necessary. Only the normal procedure for authentication is carried out.

Encryption for the baseband link requires no user input. After successful authentication and retrieval of the current link key, this function generates a new encryption key from the link key for each communication session. A stream cipher algorithm is used that is well suited to hardware implementation. The encryption key length ranges between 8 – 128 bits depending on the level of security and export regulations. In addition, the maximum encryption length is hardware-restricted.

An overview of security mode 2

In security mode 2 it is possible to define security levels for devices and services. There are two levels of trust for devices:

1) A trusted device, which has a fixed relationship (paired), is trusted and has unrestricted access to all services.

2) An untrusted device, which has no permanent fixed relationship (but possibly temporary), or which has a fixed relationship and is not trusted. Here the access to services is restricted.

A possible refinement is to set the trust level of a device specifically for services or a group of services.

For services the requirement for authorization (permitted or denied access to a service), authentication (identifying ‘who’ is at the other end of the link) and encryption are set independently. Three security levels govern service access:

1) Services that require authorization and authentication. Automatic access is only granted to trusted devices: other devices need manual authorization.

2) Services that require authentication only.

3) Services open to all devices.

A default security level is defined to serve the needs of legacy applications. This default policy will be used unless other settings are found in a “security” database related to a service, e.g., an internal security information database.

The device and service security behavior as seen from the remote device is specified in the Generic Access Profile in volume 2 of the Bluetooth Specification [1]. Implementation guidelines can also be found in the white paper [2]. The approach described there introduces a security manager, which is queried during connection establishment. The principle is illustrated in Figure 3. The security manager decides on access based on the

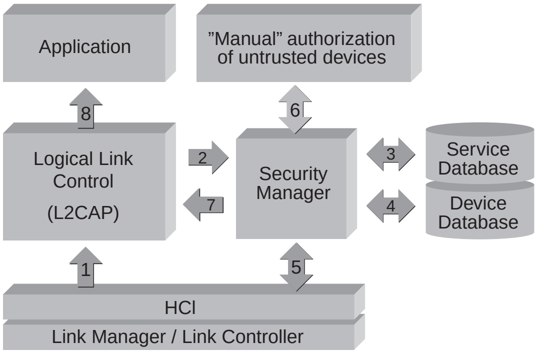

Application
”Manual” authorization of untrusted devices
8
6
Logical Link Control (L2CAP)
2
7
Security Manager
3
4
Service Database
Device Database
1
5
HCI
Link Manager / Link Controller

Figure 3. Processing of an access request by the security manager in security mode 2.

trust level of the device and the security level of the service – both taken from internal databases.

Bluetooth security is not intended to replace existing network security features. For extremely high or special requirements (e.g. e-commerce or personalized instead of device-oriented authorization) additional application-level security mechanisms can be implemented. In the Bluetooth profiles this approach has already been used for synchronization, where OBEX authentication is used.

References:

[1] Bluetooth Specification 1.0, especially sections B:14, C:1-3 and K:1.

[2] Bluetooth Security Architecture White Paper, http://www.bluetooth.com.

[3] Thomas Müller: Bluetooth Security. Bluetooth'99, London, June 1999.

[4] Joakim Persson: Bluetooth Baseband Security Concept. Bluetooth'99, London, June 1999.

Bluetooth Compliance Update

The Bluetooth promise, "Wireless Connections Made Easy," is built on different products working together flawlessly. With many of our 1000 Adopters developing Bluetooth products, the only sure way to deliver on that promise is to make certain that every product complies with the specification (Volume 1, part I:2).

Every Bluetooth product must complete the Bluetooth Qualification process. This process calls for product testing by the manufacturer and by a Bluetooth Qualification Test Facility (BQTF); and for reviews by a Bluetooth Qualification Body (BQB) of test reports, product documents, and manufacturer declarations. Conformance and interoperability testing will be required on protocol and profile levels. The qualification testing requirements will be identified through the test case reference list, which is the list of currently applicable test cases.

While test specifications and test systems are being developed, we initially rely on interoperability tests with "Golden Units" produced by Nokia and Ericsson, as well as the manufacturers' records of performing defined conformance test cases. Additionally, the manufacturer must issue a signed Declaration of Compliance. As conformance test systems become available, records of standardized executable conformance tests will be required instead of manufacturers' implementations of the related abstract test suites.

Don't forget that every Bluetooth product must be on the Bluetooth Qualified Products List to be properly licensed, so contact a BQB early for details on current listing requirements.

Stay tuned for more announcements about Bluetooth Qualification activities soon, including the first interoperability event (being planned for later this year), Bluetooth Qualification Web pages (where you'll find the Declaration of Compliance form and details on product qualification requirements), BQB appointments, and other news.

Share your experience

In future issues of the Bluetooth SIGnal we would like to present stories on how SIG members are applying (or intend to apply) the Bluetooth technology to their products. Therefore if you think that you have an interesting application story to tell, including the challenges involved and how you are meeting them, contact us at bluetooth@pyramid.se.

COMING UP

Sept 22–24
PCS, New Orleans

Oct 10–17
Telecom 99, Geneva

Nov 1–5
Embedded Systems, San Jose, California

Nov 8–10
IIR Bluetooth Conference, Amsterdam

Nov 15–19
Comdex, Las Vegas

Dec 6–9
Bluetooth Developers Conference, Los Angeles

Bluetooth SIGnal is the offical newsletter of the Bluetooth Special Interest Group (SIG).

It is sponsored by:
Ericsson
IBM
Intel
Nokia
Toshiba

The next Bluetooth SIGnal will be published on Nov 26.

The newsletter is produced by Pyramid Communication AB for the Bluetooth SIG 1999 ©.

Suggestions and feedback on articles are welcomed at bluetooth@pyramid.se