Find Me Profile

Abstract

The Find Me profile defines the behavior when a button is pressed on one device to cause an alerting signal on a peer device.

Revision History

Revision	Date	Comments
D09r01	2010-05-10	First Draft of Find Me Profile
D09r02	2010-05-17	Minor corrections
D09r03	2010-05-19	Comment from Frank Berntsen
D09r04	2010-11-29	Updated to align with approved UCRDD
D09r05	2010-12-01	Edited on WG call. Resolved comments
D09r06	2010-12-10	Changes to align document structure
D09r07	2010-12-13	Changes from Jason Hillyard; section 6 corrections
D07r08	2010-12-15	Comments from TB & responses
D07r09	2010-12-16	Further BARB comments (TB, DT, TH) & responses
D07r10	2010-12-17	Version approved by BARB on 16/Dec
D10r01	2011-02-06	Draft 1.0 version (no changes)
D10r02	2011-04-14	Added LE Connection Establishment section.
D10r03	2011-04-20	Additional text added to section 4.3.
D10r04	2011-05-17	Updates to section 5
D10r05	2011-06-07	Removed BR/EDR
D10r06	2011-06-15	Update to security to avoid slave security request before bonded. 4 editorials in section 5.
D10r07	2011-06-16	Removed conditional "if bond" and the unnecessary sentence "should bond during this procedure".
V10r00	2011-06-21	Adopted by Bluetooth SIG Board of Directors.

Contributors

Name	Company
Robin Heydon	CSR plc
Nick Hunn	CSR
Kanji Kerai	Nokia
Steve Davies	Nokia
Tim Howes	Accenture
Jonathan Tanner	Nokia
Frank Berntsen	Nordic Semiconductor
Jason Hillyard	Wicentric

Disclaimer and Copyright Notice

The copyright in this specification is owned by the Promoter Members of Bluetooth® Special Interest Group (SIG), Inc. ("*Bluetooth* SIG"). Use of these specifications and any related intellectual property (collectively, the "Specification"), is governed by the Promoters Membership Agreement among the Promoter Members and *Bluetooth* SIG (the "Promoters Agreement"), certain membership agreements between Bluetooth SIG and its Adopter and Associate Members (the "Membership Agreements") and the *Bluetooth* Specification Early Adopters Agreements (1.2 Early Adopters Agreements) among Early Adopter members of the unincorporated *Bluetooth* SIG and the Promoter Members (the "Early Adopters Agreement"). Certain rights and obligations of the Promoter Members under the Early Adopters Agreements have been assigned to Bluetooth SIG by the Promoter Members.

Use of the Specification by anyone who is not a member of *Bluetooth* SIG or a party to an Early Adopters Agreement (each such person or party, a "Member"), is prohibited. The legal rights and obligations of each Member are governed by their applicable Membership Agreement, Early Adopters Agreement or Promoters Agreement. No license, express or implied, by estoppel or otherwise, to any intellectual property rights are granted herein.

Any use of the Specification not in compliance with the terms of the applicable Membership Agreement, Early Adopters Agreement or Promoters Agreement is prohibited and any such prohibited use may result in termination of the applicable Membership Agreement or Early Adopters Agreement and other liability permitted by the applicable agreement or by applicable law to *Bluetooth* SIG or any of its members for patent, copyright and/or trademark infringement.

THE SPECIFICATION IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, SATISFACTORY QUALITY, OR REASONABLE SKILL OR CARE, OR ANY WARRANTY ARISING OUT OF ANY COURSE OF DEALING, USAGE, TRADE PRACTICE, PROPOSAL, SPECIFICATION OR SAMPLE.

Each Member hereby acknowledges that products equipped with the *Bluetooth* technology ("*Bluetooth* products") may be subject to various regulatory controls under the laws and regulations of various governments worldwide. Such laws and regulatory controls may govern, among other things, the combination, operation, use, implementation and distribution of *Bluetooth* products. Examples of such laws and regulatory controls include, but are not limited to, airline regulatory controls, telecommunications regulations, technology transfer controls and health and safety regulations. Each Member is solely responsible for the compliance by their *Bluetooth* Products with any such laws and regulations and for obtaining any and all required authorizations, permits, or licenses for their *Bluetooth* products related to such regulations within the applicable jurisdictions. Each Member acknowledges that nothing in the Specification provides any information or assistance in connection with securing such compliance, authorizations or licenses**. NOTHING IN THE SPECIFICATION CREATES ANY WARRANTIES, EITHER EXPRESS OR IMPLIED, REGARDING SUCH LAWS OR REGULATIONS.**

ALL LIABILITY, INCLUDING LIABILITY FOR INFRINGEMENT OF ANY INTELLECTUAL PROPERTY RIGHTS OR FOR NONCOMPLIANCE WITH LAWS, RELATING TO USE OF THE SPECIFICATION IS EXPRESSLY DISCLAIMED. BY USE OF THE SPECIFICATION, EACH MEMBER EXPRESSLY WAIVES ANY CLAIM AGAINST *BLUETOOTH* SIG AND ITS PROMOTER MEMBERS RELATED TO USE OF THE SPECIFICATION.

Bluetooth SIG reserve the right to adopt any changes or alterations to the Specification as it deems necessary or appropriate.

Copyright © 2001 - 2011. *Bluetooth* SIG Inc. All copyrights in the Bluetooth Specifications themselves are owned by Ericsson AB, Lenovo (Singapore) Pte. Ltd., Intel Corporation, Microsoft Corporation, Motorola Mobility, Inc., Nokia Corporation, and Toshiba Corporation.

*Other third-party brands and names are the property of their respective owners.

Document Terminology

The Bluetooth SIG has adopted Section 13.1 of the IEEE Standards Style Manual, which dictates use of the words ``shall'', ``should'', ``may'', and ``can'' in the development of documentation, as follows:

The word *shall* is used to indicate mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (*shall* equals *is required to*).

The use of the word *must* is deprecated and shall not be used when stating mandatory requirements; *must* is used only to describe unavoidable situations.

The use of the word *will* is deprecated and shall not be used when stating mandatory requirements; *will* is only used in statements of fact.

The word *should* is used to indicate that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required; or that (in the negative form) a certain course of action is deprecated but not prohibited (*should* equals *is recommended that*).

The word *may* is used to indicate a course of action permissible within the limits of the standard (*may* equals *is permitted*).

The word *can* is used for statements of possibility and capability, whether material, physical, or causal (*can* equals *is able to*).

Table of Contents

1   Introduction

The Find Me profile defines the behavior when a button is pressed on a device to cause an immediate alert on a peer device. This can be used to allow users to find devices that have been misplaced.

This profile meets the use cases defined in the Find Me UCRDD [2].

1.1 Profile Dependency

This profile requires the Generic Attribute Profile (GATT).

1.2 Conformance

If conformance to this profile is claimed, all capabilities indicated as mandatory for this profile shall be supported in the specified manner (process-mandatory). This also applies for all optional and conditional capabilities for which support is indicated. All mandatory capabilities, and optional and conditional capabilities for which support is indicated, are subject to verification as part of the Bluetooth qualification program.

1.3 Bluetooth Specification Release Compatibility

This specification can be used with any version of the Bluetooth Core Specification that allows Generic Attribute Profile.
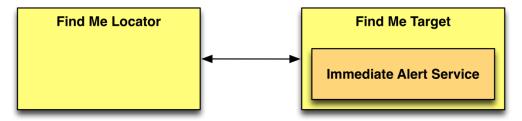
2 Configuration

2.1 Roles

The profile defines two roles: Find Me Locator and Find Me Target.

- The Find Me Target shall be a GATT server.
- The Find Me Locator shall be a GATT client.

2.2 Role / Service Relationships

The diagram below shows the relationship between services and the two profile roles.

The Find Me Target has an instance of the Immediate Alert service.

2.3 Concurrency

A device may implement a Find me Target or a Find Me Locator together with other profiles at the same time.

A device may also implement both a Find Me Target and Find Me Locator at the same time.

2.4 Topology

This profile does not impose any GAP role restrictions.

3 Find Me Target Requirements

The Find Me Target shall have only one instance of the Immediate Alert service.

	Find Me Target
Immediate Alert service	M

3.1 Immediate Alert Service

This profile does not impose any additional requirements beyond those defined by the Immediate Alert Service Specification [3].

4 Find Me Locator Requirements

The Find Me Locator shall support the Immediate Alert service [3].

This section describes the procedure requirements for a Find me Locator.

	Procedure	Ref.	Support in Find me Locator
1.	Service Discovery	4.1	M
2.	Characteristic Discovery	4.2	M
3.	Alerting Peer Device	4.3	M

Table 4.1: Find Me Locator requirements

4.1 Service Discovery

The Find Me Locator shall perform service discovery using the GATT Discover All Primary Services sub-procedure or the GATT Discover Primary Services by Service UUID sub-procedure as follows:

- To discover the Immediate Alert service with «Immediate Alert» for the service UUID.

Recommended connection parameters for LE connection establishment are defined in Section 5.

4.2 Characteristic Discovery

The GATT sub-procedure Discover All Characteristic of a Service shall be used to discover the characteristics of the following services:

- Immediate Alert service

4.3 Alerting Peer Device

When the Find Me Locator device wishes to cause an alert on the Find Me Target device, it shall write the specific Alert Level in the Alert Level characteristic. If a link does not exist then the Find Me Locator device shall connect to the Find Me Target device as defined in Section 5. The Find Me Locator device should disconnect the link after alerting the device to save battery power.

5   Connection Establishment

This section describes the connection establishment procedures used by a Find Me Target and Find Me Locator. Since there are no topology restrictions imposed by this profile, the procedures are described in terms of GAP Peripheral role (referred to as the Peripheral) and GAP Central role (referred to as the Central).

5.1   GAP Peripheral Role

5.1.1   Device Discovery

A Peripheral shall enter the GAP Limited Discoverable Mode when commanded by the user to discover a Central. The T_{GAP} (lim_adv_timeout) used during GAP *Limited Discoverable Mode* may be larger than the value specified in the Section 16, Appendix A in the GAP Specification [1], but the value shall be less than or equal to 180 seconds.

5.1.2   Connection Procedure for Unbonded Devices

This procedure is used for device discovery and connection establishment when the Peripheral is unbonded and the user initiates a connection.

It is recommended that the Peripheral advertises using the parameters in Table 5.1. The interval values in the first row are designed to attempt fast connection during the first 30 seconds; however, if a connection is not established within that time, the interval values in the second row are designed to reduce power consumption for devices that continue to advertise.

Advertising Duration	Parameter	Value
First 30 seconds (fast connection)	Advertising Interval	20 ms to 30 ms
After 30 seconds (reduced power)	Advertising Interval	1 s to 2.5 s

Table 5.1: Recommended advertising interval values

The advertising interval and time to perform advertising should be configured with consideration for user expectations of connection establishment time.

The Peripheral shall accept any valid values for connection interval and connection latency.

If a connection is not established within a time limit defined by the Peripheral, the Peripheral may exit the GAP Connectable Mode.

The Peripheral should write the Bluetooth device address of the Central in the Peripheral controller's white list and set the Peripheral controller's advertising filter policy to 'process scan and connection requests only from devices in the White List.'

5.1.3   Connection Procedure for Bonded Devices

This procedure is used after the Peripheral has bonded with the Central device using the connection procedure in Section 5.1.2 when the user initiates a connection.

A Peripheral shall enter the GAP Undirected Connectable Mode when commanded by the user to initiate a connection to a Central device.

The Peripheral should use the advertising filter policy configured when bonded using the connection procedure in Section 5.1.2.

The Peripheral should use the recommended advertising interval values shown in Table 5.1.

The advertising interval and time to perform advertising should be configured with consideration for user expectations of connection establishment time.

The Peripheral shall accept any valid values for connection interval and connection latency set by the Central until service discovery, bonding and encryption is complete. Only after that should the Peripheral change to the preferred connection parameters that best suits its use case.

If a connection is not established within a time limit defined by the Peripheral, the Peripheral may exit the GAP connectable mode.

5.1.4 Link Loss Reconnection

When a connection is terminated due to link loss a Peripheral should attempt to reconnect to the Central by entering a GAP connectable mode using the recommended advertising interval values shown in Table 5.1.

5.2 GAP Central Role

5.2.1 Device Discovery

The Central should use the GAP Limited Discovery Procedure to discover a Peripheral.

5.2.2 Connection Procedure for Unbonded Devices

This procedure is used for device discovery and connection establishment when the Central is unbonded and the user initiates a connection.

The scan interval and scan window should be configured with consideration for user expectations of connection establishment time.

It is recommended that the Central scans using the scan interval and scan window values in Table 5.2.

Parameter	Value
Scan Interval	30ms to 60ms*
Scan Window	30ms

Table 5.2: Recommended scan interval and scan window values

* During the first 30 seconds, a scan interval of 60ms is recommended when the Central is supporting other operations to provide a 50% scan duty cycle versus 100% scan duty cycle.

The Central should write the Bluetooth device address of the Peripheral in the Central controller's white list and set the Central controller's initiator filter policy to 'process connectable advertisement packets.'

Find Me Profile

5.2.3 Connection Procedure for Bonded Devices

This procedure is used after the Central has bonded with the Peripheral using the connection procedure in Section 5.2.2 when the user initiates a connection.

A Central should use a GAP connection establishment procedure to initiate a connection to a Peripheral when commanded by the user. The scan interval and scan window should be configured with consideration for user expectations of connection establishment time.

The Central should use the recommended scan interval and scan window values shown in Table 5.3. For the first 30 seconds (or optionally continuously for mains powered devices), the Central should use the first scan window / scan interval pair to attempt fast connection. However, if a connection is not established within that time, the Central should switch to one of the other scan window / scan interval options as defined below to reduce power consumption.

Scan Duration	Parameter	Value
First 30 seconds (fast connection)	Scan Interval	30ms to 60ms*
	Scan Window	30ms
After 30 seconds (reduced power) - Option 1	Scan Interval	1.28s
	Scan Window	11.25ms
After 30 seconds (reduced power) - Option 2	Scan Interval	2.56s
	Scan Window	11.25ms

Table 5.3: Recommended Scan Interval and Scan Window Values

Option 1 in the table above uses the same background scanning interval used in BR/EDR so the power consumption for LE will be similar to the power consumption used for background scanning on BR/EDR. Option 2 uses a larger background scanning interval (e.g. twice as long) than used in BR/EDR so the power consumption for LE will be significantly less than the power consumption used for background scanning on BR/EDR. Connection times during background scanning will be longer with Option 2.

The Central should use a scan window and scan interval suitable to its power and connection time requirements. Increasing the scan window increases the power consumption, but decreases the connection time.

The scan interval and scan window should be configured with consideration for user expectations of connection establishment time.

If the Central has a bond with the Peripheral, the Central shall start encryption at connection creation. If encryption fails (the bond in the Peripheral may have been deleted), the Central must, after user interaction, re-bond, perform service discovery (unless the Central had previously determined that the Peripheral did not have the «Service Changed» characteristic) and reconfigure the Peripheral before using any of the services referenced by this profile in case the configuration was altered or lost.

Find Me Profile

5.2.4 Link Loss Reconnection

When a connection is terminated due to link loss a Central should attempt to reconnect to the Peripheral using any of the GAP connection procedures and using the recommended parameters shown in Table 5.3.

5.2.5 Fast Connection Interval

To avoid very long service discovery and encryption times, the Central should use the connection intervals defined in Table 5.4 in the connection request.

Parameter	Value
Minimum Connection Interval	50 ms
Maximum Connection Interval	70 ms

Table 5.4: Recommended Connection Interval Values

At any time a key refresh or encryption setup is required, this should be preceded with a connection parameter update to a minimum connection interval of 50ms and a maximum connection interval of 70 ms and a latency of zero. This fast connection interval should be maintained until the procedure is complete and only then revert back to the preferred connection parameters as defined by the Peripheral.

6 Security and Privacy Considerations

6.1 Security Considerations

This section describes the security requirements for a Find Me Target and Find Me Locator for LE transport. Since there are no topology restrictions imposed by this profile, the requirements are described in terms of GAP Peripheral role (referred to as the Peripheral) and GAP Central role (referred to as the Central).

The Peripheral shall support LE Security Mode 1 and Security Levels 2 or 3. The Peripheral should use the SM Slave Security Request procedure only when bonded with the Central to inform the Central of its security requirements.

The Central shall support LE Security Mode 1 and Security Levels 2 and 3. The Central should accept the LE Security Mode and Security Level combination requested by the Peripheral.

6.2 Privacy

It is recommended that key fobs and watches implementing the Find Me Target role should support private addressing and reconnect address characteristic as defined in GAP.

7 GATT Interoperability Requirements

The following GATT sub-procedures are required to be implemented for both the Find Me Locator and Find Me Target roles.

GATT sub-procedure	Find Me Locator	Find Me Target
Discover All Primary Services	C.1	M
Discover Primary Services by Service UUID	C.1	M
Discover All Characteristic of a Service	M	M
Write Without Response	M	M
C.1: Either Discover All Primary Services or Discover Primary Services By Service UUID shall be supported by the Find Me Locator.		

Find Me Profile

8 Acronyms and Abbreviations

Acronyms and Abbreviations	Meaning
BR/EDR	Basic Rate / Enhanced Data Rate
GAP	Generic Access Profile
GATT	Generic Attribute Profile
LE	Low Energy
SDP	Service Discovery Protocol
UUID	Universally Unique Identifier

9 References

[1]   Bluetooth Core Specification v4.0
[2]   Find Me UCRDD
[3]   Immediate Alert Service